Confa
Contigo, con todo

Socialización

Diagnóstico Sistema de Gestión de Seguridad de la Información

Fecha: Enero 31 de 2023
Gerencia: Tecnología

¿Qué hace el Proyecto SGSI (Sistema de Gestión de Seguridad de la Información)?

Permite a una organización **analizar** y **ordenar la estructura de los sistemas de información** , facilitando la **definición de procedimientos** de trabajo para mantener su seguridad.

Fase 1: Diagnóstico (gap)
Fase 2: Cierre de brechas

**** NOTA:***
El informe gap fue diseñado y elaborado por Identian en Diciembre 2022.

Contexto del proyecto SGSI

El Proyecto Análisis, diseño e implementación del Sistema de Gestión de Seguridad de Información consta de 2 fases, la primera tiene como objetivo generar un diagnóstico de la situación actual de Confa frente a los modelos de seguridad de la información de la norma NTC-ISO-IEC 27001:2013 y MSPI del Mintic y una segunda fase de implementación donde se busca una remediación de brechas identificadas.

El proyecto inició en el mes de abril de 2022, se contrató el consultor Identian con el fin de ejecutar la fase 1, el objetivo de esta presentación es mostrar los resultados de este diagnóstico y las actividades necesarias para la remediación de brechas.

Nivel de madurez

No Existente : No hay procesos de control reconocidos. La organización no reconoce el problema y por ende la necesidad de su tratamiento.

Inicial / Ad hoc : La organización reconoce un problema que debe ser tratado. No existen procesos estandarizados sino procedimientos particulares aplicados a casos individuales.

Repetible pero intuitivo : Se desarrollan procesos para ser aplicados por personas diferentes entendiendo las mismas tareas. No hay comunicación ni entrenamiento formal y la responsabilidad recae sobre los individuos. Excesiva confianza en el conocimiento de los individuos, por tanto, los errores son comunes.

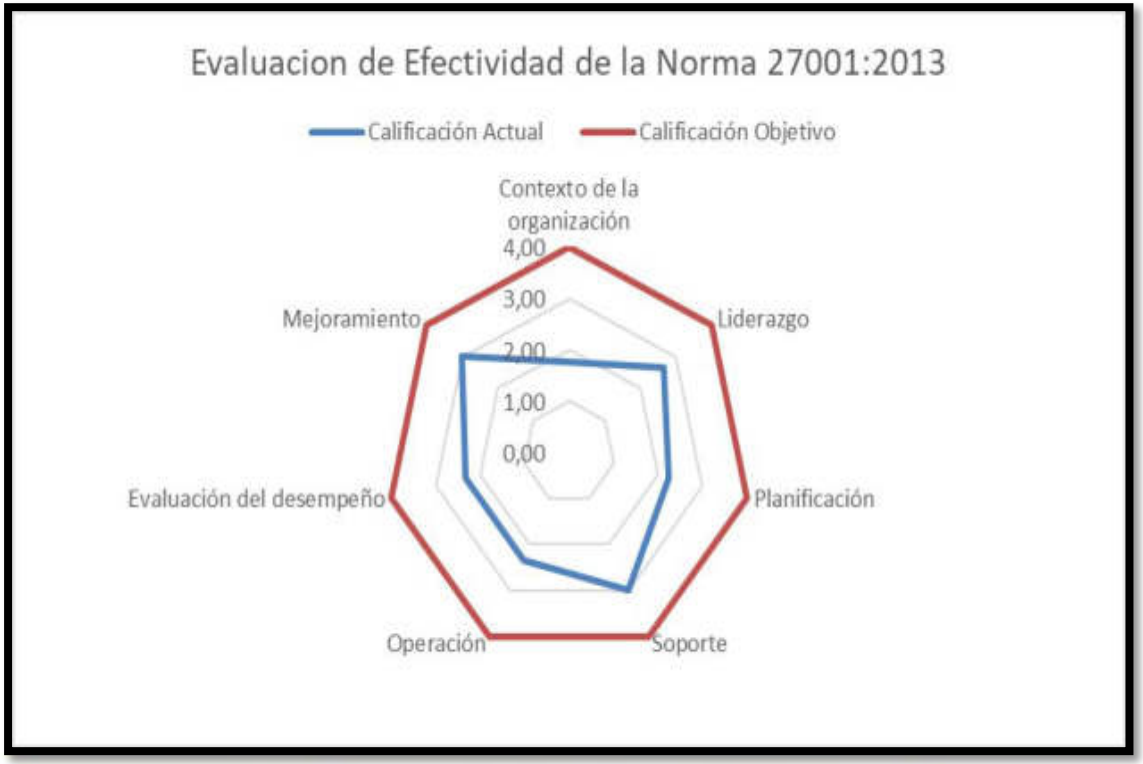
Procesos definidos : Los procesos se definen, documentan y se comunican a través de entrenamiento formal. Es obligatorio el cumplimiento de los procesos y por tanto la posibilidad de detectar desviaciones es alta. Los procedimientos por sí mismos no son sofisticados, pero se formalizan las prácticas existentes..

Administrados y medibles : Existen mediciones y monitoreo sobre el cumplimiento de los procedimientos. Los procedimientos están bajo constante mejoramiento y proveen buenas prácticas. Normalmente requiere de herramientas automatizadas para la medición.

Optimizado : Los procesos se refinan a nivel de buenas prácticas con base en los resultados del mejoramiento continuo y los modelos de madurez de otras empresas. Normalmente se cuenta con herramientas automatizadas de work flow.

Análisis GAP

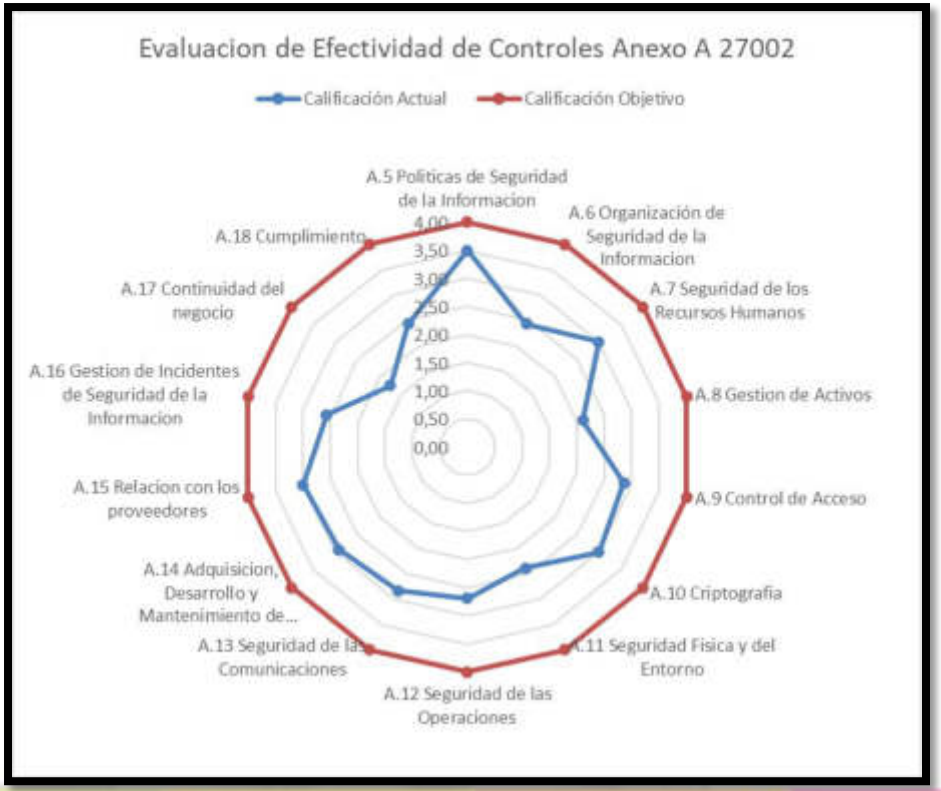
Nivel de cumplimiento de la norma :



Nivel Definido

Análisis GAP

Nivel de cumplimiento de los 114 controles del Anexo A de la norma:



Nivel Definido

VIGILADO SuperSubsidio

Planes de acción

- Actualizar la política de Seguridad de la información
- Definir estrategia para lograr que el rol de Seguridad de la información no pertenezca al área de Tecnología
- Involucrar a Seguridad de la Información en el diseño, contratación y ejecución de todos los proyectos
- Evaluar todas las capacitaciones en Seguridad de la Información
- Garantizar que el personal de Servicios Generales y Vigilancia reciban capacitación en Seguridad de la información
- Definir metodología para la gestión de activos de información
- Automatizar el control de dispositivos externos
- Definir esquema de claves a nivel organizacional

Planes de acción

- Definir áreas seguras para implementación de controles
- Documentar otros procedimientos de infraestructura
- Implementar logs centralizados
- Definir inventario de software actualizado
- Definir procedimiento para transferencia de información con terceros
- Implementar política de desarrollo de software seguro
- Realizar análisis de vulnerabilidad a toda la infraestructura
- Definir un Plan de Continuidad de Negocio
- Definir un Plan de Contingencia