# Sistemas de Seguridad de la Información

# 1. Gobierno de la seguridad

1.1 ¿Existe una función/área encargada de garantizar la seguridad de la información?

- Estructura del area de seguridad de la informacion

1.2 ¿Está alineada la seguridad de la información con la estrategia de negocio para apoyar los objetivos organizacionales?

- El gobierno de seguridad de la información incluye los elementos que se requieren para brindar a la alta dirección la certeza de que su dirección y empeño se reflejan en la postura de seguridad de la organización al utilizar un enfoque estructurado para implementar un programa de seguridad

1.3 Se ejecutan medidas apropiadas para mitigar los riesos y reducir el posible impacto que tendrían en los recursos de información a un nivel aceptable?

1.4 ¿Se realizan evaluaciones periódicamente que permitan conocer el estado del SGSI respecto a las mejores prácticas?

1.5 ¿Se conocen y planifican las inversiones y costos necesarios para alcanzar el nivel de seguridad adecuado?

- Se cuenta con presupuesto para el área de seguridad o es el mismo que se tiene para la dirección de tecnología.

# 2. Politicas y cumplimiento

2.1 ¿Se tiene creada y se mantiene la política de seguridad para la organización?

- Documento que establece las políticas que integran el Sistema de Gestión de Seguridad de la Información SGSI, las cuales deben ser adoptadas por los funcionarios, contratistas, personal interno, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la organizacion enfocado al cumplimiento de la normatividad legal Colombiana vigente y a las buenas prácticas de seguridad de la información como la norma ISO 27001/2013

2.2 ¿Se fomenta la adopción de una "cultura de seguridad de la información" en todos los niveles? (Concientización)?

- Campañas de sensibilización periodicas con el fin de dar a conocer los riesgos a los que los sistemas de información, los usuarios, las redes y la información en general están expuestos para generar dentro de los funcionarios buenas prácticas respecto a la seguridad de la información, estás buenas prácticas actúan de manera preventiva ayudando a la entidad a salvaguardar sus activos de información

2.3 ¿Tiene la organización clasificada la informacion de acuerdo a su criticidad? (política de clasificación de información)

- De acuerdo a la prioridad de la informacion, debería existir una clasificación que permita actuar de acuerdo a la urgencia establecida en casos de afectación de la disponibilidad y continuidad (robo de información, hackeo, phising, manipulación indebida) y evitar problemas a nivel general de la organización.Políticas que establezcan los estándares utilizados por la organización tendientes a proteger la confidencialidad de los Datos de Carácter Privado (o clasificados como tal) que se encuentran en su poder o bajo su control.

2.4 ¿Existen métricas para comprobar el resultado de los planes, procesos y controles de seguridad implantados?

- Métricas definidas tanto a nivel estratégico (progreso de los planes) como táctico y operativo (procesos y controles). Ejemplo: Porcentaje de disminución de contraseñas débiles tras la campaña de concientización; porcentaje de empleados que han recibido concientización en seguridad; porcentaje de equipos en los que se ha instalado antivirus

2.5 ¿El plan de seguridad de la información se ejecuta y prueba de acuerdo a lo definido en el SGSI?

- Resultados de las pruebas del plan de seguridad de la informacion y posibles ajustes aplicables

# 3. Riesgos e Incidentes de Seguridad

3.1 ¿Se les da tratamiento a las amenazas y vulnerabilidades que pueden poner en riesgo la seguridad de la información?

- Qué amenazas y vulnerabilidades han aumentado su exposición a riesgo los últimos 12 meses? (relacionado con el uso de redes sociales, computación en la nube, computación móvil, accesos no autorizados, empleados descuidados o inconsientes, controles de seguridad obsoletos, contraseñas)

3.2 ¿Los incidentes de seguridad reciben tratamiento diferencial respecto a los incidentes generados por la operación?

- Existe en la organización un área especializada para la gestión de incidencias de seguridad, por ejemplo un SOC.

3.3 ¿Se puede identificar la trazabilidad de los incidentes de seguridad?

- Herramienta, log o similar que muestre la traza de los incidentes para conocer la procedencia y historial de los incidentes de seguridad

# 4. Acceso y Confidencialidad

4.1 ¿La organización cuenta con herramientas de aprovisionamiento de derechos a aplicaciones y servicios según el rol, que permitan otorgar, denegar los accesos?

- Herramienta de gestion de servicios o similar para configurar y controlar los accesos

4.2 ¿Se monitorea el acceso a los servicios considerando criterios como identidad; rol; derechos?

4.3 ¿Se controla el acceso de terceros a las instalaciones, aplicaciones y servicios de la organización?

---

Revision #2
Created 21 January 2021 15:52:55 by CertMind
Updated 21 January 2021 16:11:41 by CertMind