Organización de la seguridad de la información

Objetivo del documento:

1. Este documento es un ejemplo de la manera de organizar la seguridad de la información dentro de las empresas en Colombia.
2. Este documento es sólo una guía y no una estricta regla de cumplimiento.
3. Define las directrices para gestionar la seguridad de la información dentro de SISTESEG.

Compromiso de la gerencia con la Seguridad de la Información

La gerencia o directivas de SISTESEG, debe apoyar activamente la seguridad de la información dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explicita y el conocimiento de las responsabilidades de la seguridad de la información. Este compromiso se verá reflejado a través de:

- Creación de un comité de seguridad interdisciplinario incluyendo el Área IT.
- Asignación de un responsable de la seguridad de la información(Oficial de seguridad)
- Aprobación del documento de políticas de seguridad de la información
- Velar por el cumplimiento de las políticas de seguridad de la información
- Asignación de responsabilidades asociadas al tema de la seguridad de la información

[A.6.1.1]

Funciones del Comité de Seguridad de la información

El comité de seguridad de la información debe estar conformado por miembros de alto nivel de los departamentos y Áreas de SISTESEG.

- Debe periódicamente revisar el estado general de la seguridad de la información
- Revisar y monitorear los incidentes de seguridad de la información
- Revisar y aprobar los proyectos de seguridad de la información
- Aprobar las modificaciones o nuevas políticas de seguridad de la información
- Realizar otras actividades de alto nivel relacionadas con la seguridad de la información

Por último, cuando el comité de seguridad de la información se reúna con el propósito de revisar temas de seguridad de la información se incluirá la participación del Oficial de Seguridad.

Coordinación de la Seguridad de la Información

Las actividades de la seguridad de la información deben ser coordinadas por los representantes de todas las partes de SISTESEG con roles y funciones laborales pertinentes.

[A.6.1.2]

- La gerencia de SISTESEG es responsable de que los empleados a su cargo, conozcan y apliquen las políticas de seguridad de la información.

- SISTESEG deberá contar con un Oficial de Seguridad de la Información que asuma las tareas y responsabilidades que conlleva este rol:

    - Definir y actualizar políticas, normas, procedimientos y estándares definidos en el SGSI
    - Realizar el análisis de riesgo a las aplicaciones
    - Asesorar en la aplicación de la metodología para el mantenimiento de los planes de contingencia y continuidad del negocio
    - Evaluar, seleccionar e implantar herramientas que faciliten la labor de seguridad de la información
    - Dar los lineamientos para controlar el acceso a los sistemas de información y la modificación de privilegios
    - Promover en SISTESEG la formación, educación y el entrenamiento en seguridad de la información
    - Mantenerse actualizado en nuevas amenazas y vulnerabilidades existentes
    - Recibir capacitación en el tema de seguridad de la información
    - Realizar estudios de penetración y pruebas de seguridad en todos los ambientes[1] (Desarrollo, Pruebas, Producción y Contingencia)

Asignación de responsabilidades para la Seguridad de la Información

Se deben definir claramente todas las responsabilidades en cuanto a seguridad de la información. En especial las relacionadas a la existencia de un comité de seguridad de la información y un oficial de seguridad.

[A.6.1.3]

Oficial de Seguridad de la información

SISTESEG mantendrá dentro de su planta de empleados un Oficial de Seguridad de la información, cuyas funciones estarán caracterizadas y definidas en el documento SGSI.

Comité de seguridad de la información

El Oficial de Seguridad, podrá convocar a diferentes empleados para formar grupos interdisciplinarios, que apoyen la definición e implementación de los diferentes temas de seguridad de la información.

Dueños de la Información

[1] Para esta actividad se recomienda el uso de la herramientas LanGuard de GFI.

Toda la información utilizada por SISTESEG, debe poseer un dueño. Estos dueños de la información son responsables de los activos y deben:

- Definir la clasificación de la información
- Determinar los niveles de acceso a la información
- Autorizar la asignación de permisos de acceso
- Apoyar al Área IT en la generación de los controles necesarios para el almacenamiento, procesamiento, distribución y uso de la información

La gerencia

La gerencia de SISTESEG es responsable que los empleados a su cargo, conozcan y apliquen las políticas de seguridad de la información.

Empleados

Son responsables por el cumplimiento de las políticas de seguridad de la información. Adicionalmente cada empleado está obligado a reportar al Oficial de Seguridad cualquier incidente de seguridad de la información del que tenga conocimiento.

Contratistas, proveedores y terceros

Los contratistas, proveedores y terceros que tengan acceso a los activos de información, están obligados a cumplir las políticas de Seguridad de la Información de SISTESEG.

Administradores de los sistemas

Los administradores de los diferentes sistemas deben en forma activa implementar las normas, estándares, formatos y procedimientos, para brindar un nivel apropiado de seguridad de la información.

Autorización para nuevos servicios de procesamiento de la Información

Se debe definir e implementar un procedimiento de autorización de la gerencia para nuevos servicios de procesamiento de la información.

[A.6.1.4]

Se debe considerar para esta implementación los siguientes aspectos:

- La asignación de un dueño para cualquier nuevo servicio a implementar, además incluyendo la definición de las características de la información, tales como clasificación y definición de los diferentes niveles de acceso por usuario.
- El dueño de la información debe explícitamente dar autorización para usar este nuevo servicio.
- Se debe contar con la autorización respectiva por parte del oficial de seguridad de la información, garantizando que el nuevo servicio cumple con las políticas de seguridad de la información definidas en este documento.
- Evaluar la compatibilidad a nivel de hardware y software con otros sistemas.

- Identificar las vulnerabilidades que genere el nuevo servicio y además definir los controles necesarios para mitigarlas.

Acuerdos de confidencialidad

Se debe identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no divulgación que reflejan las necesidades de SISTESEG para la protección y seguridad de la información.

[A.6.1.5]

Todos los empleados de SISTESEG, contratistas, proveedores y terceros, que deban realizar labores dentro de SISTESEG, ya sea por medios lógicos o físicos que involucren el manejo de información, deben conocer, entender, firmar y aceptar el correspondiente acuerdo de confidencialidad de la información, para empleados y terceros Contactos con las autoridades.

[A.6.1.6]

Revisión independiente de la Seguridad de la Información.

Las políticas de seguridad de la información, normas, controles, estándares, formatos y procedimientos, deben ser revisados periódica y planificadamente, por un área independiente de sistemas dentro de SISTESEG o por un organismo o consultor externo. Este periodo debe ser de al menos *una vez al año* o cada vez que ocurra un cambio sustancial en la infraestructura o activos de información de la organización. La auditoría requerida seguirá los linimientos ISO 27001, realizada por alguien con las credenciales de AUDITOR LIDER (Lead Auditor) 27001 vigentes o Auditor CISA.

[A.6.1.8]