SEGURIDAD DE LA INFORMACIÓN: ROLES, RESPONSABILIDADES Y AUTORIDADES

1. Comité de Gobierno Digital:

Las funciones del Comité de Gobierno Digital están establecidas en la Resolución Ministerial N.° 087-2019-PCM:

- Gestionar la asignación de personal y recursos necesarios para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en sus Planes Operativos Institucionales, Plan Anual de Contrataciones y otros.
- Promover y gestionar la implementación de estándares y buenas prácticas en seguridad digital en la entidad.
- Elaborar informes anuales que midan el progreso de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI).
- Vigilar el cumplimiento de la normatividad relacionada con la implementación de seguridad de la información en las entidades públicas.
- Gestionar, mantener y documentar el Sistema de Gestión de la Seguridad de la Información (SGSI).
- Promover la conformación de equipos multidisciplinarios ágiles para la implementación de proyectos e iniciativas de digitalización de manera coordinada con los responsables de órganos y unidades orgánicas de la entidad

2. Oficial de seguridad de la información

- Elaborar las propuestas de actualización de los documentos del SGSI.
- Custodiar la información documentada del SGSI.
- Coordinar los programas de auditoría interna y externa del SGSI.
- Presentar los hallazgos de las auditorías.
- Presentar los avances de la atención de los hallazgos de Auditorías.
- Coordinar la realización periódica del proceso de evaluación de riesgos con los responsables de los procesos incluidos en el alcance del SGSI.
- Presentar los resultados de los indicadores del SGSI al Comité de Gobierno Digital para su evaluación.
- Coordinar la atención de los incidentes de Seguridad de la Información.
- Coordinar la ejecución de pruebas de análisis de vulnerabilidades informáticas en la infraestructura tecnológica.

SEGURIDAD DE LA INFORMACIÓN: ROLES, RESPONSABILIDADES Y AUTORIDADES

3. Los propietarios de los activos de información

- Clasificar sus activos de información en relación a los criterios de confidencialidad, integridad y disponibilidad.
- Mantener actualizado la clasificación de su inventario de activos.
- Definir los niveles de acceso a sus activos de información y realizar la revisión periódica de estos con la finalidad de protegerlos de un acceso no autorizado.
- En general, tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

4. Los propietarios de los riesgos

- Responsables de gestionar la ejecución del plan de tratamiento de riesgos.
- Realizar actividades e implementar controles con la finalidad de mantener los riesgos a su cargo dentro de los niveles de aceptación definidos por el OSIPTEL.

5. Usuarios de activos de información

- Todo colaborador y tercero que use o tenga acceso a los activos de información de OSIPTEL son responsables de conocer y cumplir las Políticas de Seguridad de la Información PO-SGSI-001.

¡Nuestra información está segura!