ESE ALEJANDRO PRÓSPERO REVEREND

REGLAMENTO INTERNO COMITÉ SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Santa Marta D.T.C.H - Magdalena

Mayo, 2023

CONTROL DE CAMBIOS			
Nombre del documento	Reglamento Interno Comité Seguridad y Privacidad de la Información		
Descripción del cambio		Fecha de cambio	Versión creada
Codificación de dicho documento – Versión inicial		31-may-2023	1

Avenida del Libertador 25 - 67
gerencia@esealproreu.gov.co
www.esealproreu.gov.co
intranetesealproreu
Nit: 819.004.070-5

Contenido

Avenida del Libertador 25 - 67
gerencia@esealproreu.gov.co
www.esealproreu.gov.co
intranetesealproreu
Nit: 819.004.070-5

1. INTRODUCCIÓN

El presente documento regula la conformación y el funcionamiento del Comité de Seguridad de la Información, destinado a garantizar el apoyo a las directivas de la Empresa Social del Estado Alejandro Próspero Reverend en la implementación del Modelo de Seguridad y Privacidad de la Información, así mismo en la gestión de los Riesgos de Seguridad de la información, y el mantenimiento de los mismos. Buscando de esta manera resguardar los datos de la institución, los pacientes y trabajadores, garantizando la confiabilidad, disponibilidad y seguridad de la información.

2. OBJETIVO DEL REGLAMENTO DEL COMITÉ DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Establecer los roles y responsabilidades de los integrantes del comité de seguridad y privacidad de la información de la ESE Alejandro Próspero Reverend.

3. CONFORMACIÓN

El comité de Seguridad y Privacidad de la Información de la ESE Alejandro Próspero Reverend, estará conformado así:

1. Jefe de la oficina de sistemas o su delegado.
2. El jefe de la oficina de Planeación o su representante.
3. El jefe de la oficina Jurídica o su delegado.
4. El PU oficina de Calidad o su delegado
5. El referente de la oficina de Gestión Documental o su delegado.
6. El jefe de la oficina de Control Interno o su delegado.
7. El oficial de cumplimiento de Seguridad de la información de la entidad.
8. El oficial de cumplimiento SARLAFT que tenga en su momento la entidad.

4. GESTIÓN Y FUNCIÓN

La función y gestión del comité están estipuladas por la resolución 389 del 14 de octubre del 2022 y la resolución 500 del 2021 de MINTIC.

a. Funciones

1. Coordinar la implementación del modelo de seguridad de la información al interior de la entidad.
2. Revisar los diagnósticos del estado de seguridad y privacidad de la información.
3. Acompañar e impulsar el desarrollo de proyectos de seguridad.
4. Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y

Avenida del Libertador 25 - 67
gerencia@esealproreu.gov.co
www.esealproreu.gov.co
intranetesealproreu
Nit: 819.004.070-5

objetivos con la EMPRESA SOCIAL DEL ESTADO ALEJANDRO PROSPERO REVEREND.

5. Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
6. Implementar mecanismos de gestión y monitoreo que protejan la infraestructura de TI de amenazas físicas y digitales.
7. Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
8. Participar en la formulación y evaluación de los planes de acción para mitigas y/o eliminar riesgos.
9. Realizar revisiones periódicas, SGSI (por lo menos una vez al año) y según resultados de la revisión definir las acciones pertinentes.
10. Promover la difusión y la sensibilización de la seguridad de la información dentro de la entidad.
11. Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal de la misma.
12. Las demás funciones inherentes a la naturaleza del comité.

b. Gestión

1. Definir controles considerando aspectos tales como la estructura, tamaño, canales de atención, volumen transaccional, número de usuarios, evaluación del riesgo y servicios prestados por la entidad.
2. Realizar una gestión efectiva de la seguridad de la información y la seguridad digital en la entidad.
3. Reportar los resultados del análisis de riesgos y gestión de incidentes al comité institucional de gestión y desempeño o quien haga sus veces.
4. Estar al tanto de las nuevas modalidades de ciberataques que pudieran llegar a afectar a la entidad, según las políticas que establezca la entidad de acuerdo con su evaluación de riesgo y atendiendo criterios de razonabilidad.
5. Establecer las capacitaciones que recibirán los funcionarios de la entidad en temas

Avenida del Libertador 25 - 67
gerencia@esealproreu.gov.co
www.esealproreu.gov.co
intranetesealproreu
Nit: 819.004.070-5

relacionados con seguridad digital y mantenerlos actualizados sobre las nuevas amenazas cibernéticas.

6. Realizar el monitoreo del cumplimiento de las políticas y procedimientos que se establezcan en materia de seguridad de la información y sin perjuicio de aquellas tareas que realizan las autoridades de control.
7. Asesorar a la dirección de la entidad sobre seguridad de la información y seguridad digital para que pueda hacer seguimiento y tomar las decisiones adecuadas en esta materia.
8. Realizar un análisis de riesgo para determinar la pertinencia de contratar o implementar el servicio de un equipo especializado para atender incidentes de seguridad digital. El análisis debe identificar las características del proveedor, herramientas, servicios y privacidad de la información, entre otros.
9. Determinar los recursos técnicos, humanos y administrativos de seguridad de la información y seguridad digital, necesarios para la entidad. Dichos recursos deben manejarse de manera diferenciada a los de operaciones y tecnología de la información.
10. Implementar y gestionar un Sistema de Gestión de Seguridad de la Información de acuerdo con lo establecido en el Modelo de Seguridad y Privacidad de la Información, que permita gestionar los riesgos de seguridad de la información de la entidad de una manera adecuada y oportuna.
11. Cumplir los lineamientos de gestión del riesgo establecidos en la guía para la administración del riesgo y el diseño de controles en entidades públicas expedida en el marco del modelo integrado de planeación y gestión.
12. Determinar e implementar controles de protección de la privacidad en aquellos sistemas relacionados con el tratamiento de datos personales.
13. Adoptar medidas, al momento de adquirir productos y servicios de Seguridad Digital operados en entornos de nube, que garanticen el cumplimiento de lo dispuesto en la Ley Estatutaria 1581 de 2012 y sus normas reglamentarias, en particular las relativas a la transferencia internacional de datos personales.

c. Gestión y Seguridad de la Información para Proveedores

Avenida del Libertador 25 - 67
gerencia@esealproreu.gov.co
www.esealproreu.gov.co
intranetesealproreu
Nit: 819.004.070-5

La resolución 500 del 2021 de MINTIC también establece una normatividad para la gestión y seguridad de la información con proveedores:

1. Definir claramente los roles y responsabilidades de seguridad de la información con respecto a la relación con el proveedor.
2. Propender por mantener una arquitectura de seguridad al adquirir productos o servicios de Seguridad Digital.
3. Analizar los riesgos de Seguridad Digital propios de la integración de soluciones e implementar controles para su mitigación.
4. Implementar controles que permitan minimizar los riesgos asociados a la transferencia de datos generada por cambios de fabricante o proveedor.
5. Identificar la vida útil de los productos y servicios adquiridos con el fin de planificar cualquier migración o transferencia y respaldar los datos para garantizar la continuidad de la operación.
14. Optimizar la gestión de los riesgos de Seguridad Digital estableciendo estrategias soportadas en servicios de nube.

d. Funciones Secretaría Técnica

De acuerdo con la Resolución 389 del 14 de octubre de 2022, el secretario tiene asignadas las siguientes funciones:

1. Elaborar actas de las reuniones del comité y verificar su formalización por parte de sus miembros.
2. Remitir oportunamente a los miedros la agenda de cada comité.
3. Llevar la custodia y archivo de las actas y demás documentos soporte.
4. Servir de interlocutor entre terceros y el comité.
5. Presentar los informes que requiera el comité.
6. Las demás que le sea asignadas por el comité.

e. Responsabilidades Miembros del comité

Cada integrante del Comité de Seguridad de la Información tiene ciertas responsabilidades y tareas que deben cumplir, las cuales incluyen:

1. Los miembros del Comité de Seguridad de la Información deben informar en un

Avenida del Libertador 25 - 67
gerencia@esealproreu.gov.co
www.esealproreu.gov.co
intranetesealproreu
Nit: 819.004.070-5

plazo de tres (3) días, al presidente del comité sobre cualquier situación que pueda generar una posible incompatibilidad después de haber sido designados como miembros, para tomar las medidas necesarias para evitar cualquier conflicto de interés.

2. notificar al secretario del comité con al menos 72 horas de anticipación en caso de no poder asistir a las reuniones programadas, y proporcionar una justificación adecuada mediante correo electrónico.
3. Estar informado sobre las regulaciones vigentes en materia de seguridad digital y tomar las medidas necesarias para cumplirlas.
4. Proporcionar información confidencial únicamente cuando exista requerimiento expreso, fundado y motivado de las autoridades judiciales.
5. Comprometerse a actuar con integridad y ética, y abstenerse de utilizar cualquier información confidencial o privilegiada obtenida a través de sus funciones en el Comité de Seguridad de la Información para obtener beneficios personales o en beneficio de terceros.
6. Supervisar el cumplimiento de las políticas y procedimientos de seguridad de la información establecidos, y tomar las medidas necesarias para garantizar que se respeten y se mejoren continuamente.

5. REGLAMENTO

a. Frecuencias de reuniones

Según la resolución 389 del 14 de octubre del 2022 el comité se reunirá (3) veces al año previa convocatoria del secretario técnico del comité, se podrá convocar a sesiones extraordinarias cuando sea necesario de acuerdo con temas de riesgo, incidentes o afectaciones de continuidad dentro del sistema de gestión de riesgos de la seguridad de la información.

b. Quórum

Las reuniones del Comité serán válidas cuando asista la mayoría de sus miembros con voz y voto, lo que representa la mitad más uno del total de miembros.

c. Desarrollo de sesiones

Avenida del Libertador 25 - 67
gerencia@esealproreu.gov.co
www.esealproreu.gov.co
intranetesealproreu
Nit: 819.004.070-5

Las sesiones se llevarán a cabo de la siguiente manera:

- Verificación del quórum por parte del secretario técnico.
- Lectura del orden del día.
- Lectura del acta de la sesión anterior.
- Revisión cumplimiento de los compromisos de la sesión anterior.
- Desarrollo orden del día
- Se procederá a debatir y votar sobre los temas incluidos en el orden del día.
- Lectura de compromisos generados de la sesión.

d. Elección secretario técnico del comité

En la primera sesión del comité deberá ser elegido el secretario técnico, por un período de doce (12) meses, una vez cumplido el plazo deberá elegirse un nuevo secretario al interior del comité. En caso de que el secretario del Comité no se encuentre disponible en una sesión, los miembros presentes podrán elegir de forma temporal a un secretario ad-hoc para esa reunión.

e. Votaciones

Las decisiones se tomarán por voto simple. En situaciones donde no se alcanza una mayoría de votos debido a un empate en la cantidad de miembros a favor y en contra de una decisión, se recurrirá al voto de calidad del secretario técnico del comité para tomar una decisión final. En este caso, el voto de la persona que funja como secretario tendrá un peso doble y se considerará como dos votos a favor o en contra, dependiendo de su decisión.

f. Decisiones Urgentes

En el caso de decisiones urgentes que no puedan esperar hasta la próxima sesión y deban ser ejecutadas de forma inmediata, el Comité podrá utilizar diversos medios electrónicos para llevar a cabo una votación a distancia. Los medios elegidos deberán permitir la verificación de la fecha, hora y contenido de las opiniones o decisiones expresadas por

Avenida del Libertador 25 - 67
gerencia@esealproreu.gov.co
www.esealproreu.gov.co
intranetesealproreu
Nit: 819.004.070-5

los miembros del Comité. Es importante destacar que estas decisiones deberán ser registradas en un acta y formalizadas para que sean válidas.

g. Actas

Se registrará en acta todos los asuntos debatidos y los acuerdos adoptados en las reuniones del Comité. Además, se hará constar si algún miembro se ha abstenido de participar en algún tema debido a un conflicto de intereses o por estar en contra de este.

Es fundamental que estas actas sean distribuidas con la misma anticipación que la convocatoria de la próxima sesión y que una vez aprobadas, se integren al libro de actas del Comité y se conserven por al menos 5 años. Los documentos presentados ante el Comité para su revisión, y que sean sustento de sus decisiones, deberán ser anexados a las actas. La responsabilidad de la custodia de las actas recae en el secretario del Comité, y estas deberán estar enumeradas y firmadas por los asistentes y el secretario del Comité en cada sesión.

h. Informes

Será potestad del secretario técnico del comité presentar los informes requeridos a los miembros del comité.

i. Conflicto de intereses

Los integrantes del comité que tengan conflictos de interés, en algún tema o asunto a tratar, deberán abstenerse de las liberaciones, votaciones de dicho asunto. Sin afectar el quórum.

6. DOCUMENTOS DE REFERENCIA

- Documento Maestro del Modelo de Seguridad y Privacidad de la Información, febrero 2021
- Resolución 389 del 14 de octubre del 2022

Elaboró: Adriana Ariza Monsalve, profesional Universitario Líder TIC
Revisó: Claudia Coronel Brochero, jefe Oficina Asesora de Planeación – Oficial Seguridad de la Información
Aprobó: Comité Seguridad de la Información

Avenida del Libertador 25 - 67
gerencia@esealproreu.gov.co
www.esealproreu.gov.co
intranetesealproreu
Nit: 819.004.070-5