**TITULO I**

**Artículo 6. Marco de Trabajo**

[“Utilice un marco de referencia para realizar un programa de seguridad cibernética Ejemplo: Cobit 5”, “Elabore un conjunto de mejores prácticas para en la seguridad de la Información, Medir el desempeño de las TI.”, “Organice la Tecnologías de la información conforme a los objetivos de la organización “]

[“Realice un análisis de Gestión de riesgos”, “Realice una Inventario para la identificación de activos informáticos”, “Realice una matriz de riesgos, para evaluar la probabilidad de ocurrencia y el impacto “]

[“Realice una matriz de riesgos, para evaluar la probabilidad de ocurrencia y el impacto “, “Realice un plan de control de riesgos, valoración para aceptar, mitigar, transferir o evitar la ocurrencia del riesgo”, “Monitoreo de la eficiencia y eficacia de las medidas de seguridad”]

[“Establecer una política, para la evaluación de controles existentes una vez al año, “, “establecer normas y prácticas para el cumplimiento del programa de seguridad cibernética”, “Realizar un procedimiento para la medición de controles para el programa de seguridad cibernética “]

[“, “, “]

**Artículo 7. Estructura**

[“Crear una política para asignar un encargado de la unidad funcional de seguridad cibernética”, “establecer que este cargo será ocupado por un alto ejecutivo designado por el consejo u órgano societario”, “Establecer en la política los roles del encargado de la unidad funcional de seguridad cibernética”]

[“Establecer un plan de supervisión periódica para la evaluación de la estructura de seguridad cibernética por parte del consejo u órgano societario”, “crear los lineamientos de los puntos críticos a supervisar por parte del órgano societario o consejo”, “Agendar los días y horarios de la supervisión a realizar por parte del consejo u órgano societario”]

[“Establecer en el reglamento institucional, la independencia de la estructura de seguridad cibernética en toma de decisiones, hacia cualquier otro departamento.”, “Establecer los límites de decisiones que pueda tomar la estructura de seguridad cibernética, respecto al comité u órgano societario”, “realizar evaluación del estado actual de la estructura del comité funcional de seguridad cibernética respecto a otras áreas”]

[“Establecer en el reglamento institucional que otro comité relacionado a la seguridad cibernética, tiene que tomar el cargo del comité funcional de seguridad cibernética”, “Establecer en el reglamento institucional la creación de un comité de gestión de riesgos”, “Establecer los roles y responsabilidades que el comité interino tendrá a su cargo al momento de no existir un comité funcional se seguridad cibernética”]

[“, “, “]

**Artículo 8. Aprobación del programa de Seguridad Cibernética y de la Información**

[“Establecer en el Reglamento institucional que, todo desarrollo e implementación de una nueva política, debe ser sometido a aprobación por el consejo u órgano societario”, “Crear una política que establezca la implementación de nuevas políticas del programa de seguridad cibernética.”, “Crear un procedimiento para el desarrollo de políticas para el programa de seguridad cibernética”]

[“Establecer los roles y responsabilidades del Comité funcional del programa de seguridad cibernética”, “Crear procedimientos para la asignación de responsabilidades y roles al comité funcional del programa de seguridad cibernética”, “Crear controles para supervisar el nivel de madurez del comité funcional del programa de seguridad cibernética, respecto a responsabilidades y roles”]

[“Crear un procedimiento para el desarrollo de políticas para el programa de seguridad cibernética”, “crear un control para el cumplimiento de los procedimientos para aprobación de nuevos reglamentos”, “monitorear los controles para el cumplimiento de procedimientos para aprobación de nuevos reglamentos”]

[“Crear una política que establezca el tiempo adecuado entre aprobación e implementación de un nuevo reglamento”, “Establecer sanciones en la política si existe incumplimiento de tiempo, para la implementación de nuevo reglamento”, “Crear un procedimiento para la aprobación e implementación de nuevo reglamentos”]

[“Establecer sanciones en la política de nuevos reglamentos, si existiera incumplimiento de tiempo en su implementación.”, “Establecer un procedimiento para la implementación de nuevos reglamentos”, “Establecer controles para el cumplimiento de nuevos reglamentos”]

**Artículo 9. Responsabilidades del Comité Funcional de Seguridad Cibernética y de la Información**

[“Establecer procedimientos para el desarrollo del programa de seguridad cibernética”, “establecer un control para el desarrollo del programa de seguridad cibernética y sus lineamientos”, “monitorear el cumplimiento de los controles para el desarrollo del programa de seguridad cibernética”]

[“Crear un procedimiento para el desarrollo de políticas para el programa de seguridad cibernética”, “crear un control para el cumplimiento de los procedimientos para aprobación de nuevos reglamentos”, “monitorear los controles para el cumplimiento de procedimientos para aprobación de nuevos reglamentos”]

[“Crear los controles para la evaluación de efectividad del programa de seguridad cibernética”, “Monitorear el cumplimiento de controles para medir la efectividad del programa de seguridad cibernética”, “Realizar documentación sobre el cumplimiento de los controles y el nivel de efectividad “]

[“Crear una política que defina que el comité funcional, ratificara las decisiones del tratamiento del riesgo, presentadas por el Oficial de seguridad cibernética”, “Crear un procedimiento para el tratamiento de riesgos”, “crear controles para la evaluación del tratamiento de riesgos”]

[“Establecer en el reglamento que, las valoraciones del programa de seguridad cibernética tienen que ser comunicadas al consejo u órgano societario”, “Crear una política para establecer la comunicación entre el consejo u órgano societario y el comité funcional para la valoración del programa de seguridad”, “Crear un procedimiento para la valoración del programa de seguridad cibernética”]

[“Crear una política para establecer la comunicación entre el consejo u órgano societario y el comité funcional para la valoración del programa de seguridad”, “Crear un procedimiento para la valoración del programa de seguridad cibernética”, “Crear controles para el cumplimiento de la comunicación entre el consejo u órgano societario y el comité funcional para valoración del programa de seguridad”]

**Artículo 10. Oficial de Seguridad Cibernética y de la información**

[“Establecer una política del perfil del Oficial de la unidad funcional de seguridad cibernética”, “crear procedimientos para evaluar aptitudes y destrezas, a los interesados en este cargo”, “establecer controles para el cumplimiento de los requisitos del perfil del oficial de la unidad funcional de seguridad cibernética”]

[“establecer controles para el cumplimiento de los requisitos del perfil del oficial de la unidad funcional de seguridad cibernética”, “monitorear el cumplimiento de los requisitos con los que debe cumplir el oficial de la unidad funcional”, “monitorear el cumplimiento de los requisitos con los que debe cumplir el oficial de la unidad funcional”]

[“Establecer en el reglamento institucional, cuáles son las responsabilidades del oficial de la unidad de seguridad cibernética”, “Crear una política para establecer sanciones por incumplimiento de deberes del oficial de la unidad funcional de seguridad cibernética”, “crear controles para la medición y evaluación de responsabilidades del oficial de seguridad cibernética”]

[“Crear una política para establecer sanciones por incumplimiento de deberes del oficial de la unidad funcional de seguridad cibernética”, “crear controles para la medición y evaluación de responsabilidades del oficial de seguridad cibernética”, “evaluar periódicamente el cumplimiento de responsabilidades del oficial de la unidad funcional de seguridad cibernética”]

[“Establecer en el reglamento institucional, cuáles son las responsabilidades y roles del oficial de la unidad de seguridad cibernética”, “crear controles para la medición y evaluación de responsabilidades del oficial de seguridad cibernética”, “evaluar periódicamente el cumplimiento de responsabilidades del oficial de la unidad funcional de seguridad cibernética”]

[“Establecer una política para reportar periódicamente la situación de la infraestructura a CSIRT por parte del oficial de la unidad funcional”, “Crear un procedimiento para reportar información al CSIRT sobre la situación de la infraestructura tecnológica”, “Crear controles para supervisar la información enviada al CSIRT”]

[“Crear una política que establezca que el cargo de oficial de la unidad de seguridad cibernética puede ser desempeñado por otra persona, por corto plazo”, “crear procedimientos para evaluar aptitudes y destrezas, a la persona asignada a este cargo provisionalmente”, “crear controles para evaluar el cumplimiento de roles y responsabilidades del cargo de Oficial de la unidad de seguridad cibernética al oficial interino”]

[“Crear procedimientos para evaluar aptitudes y destrezas, a la persona asignada a este cargo provisionalmente”, “crear controles para evaluar el cumplimiento de roles y responsabilidades del cargo de Oficial de la unidad de seguridad cibernética al oficial interino”, “Monitorear constantemente la efectividad del Oficial interino respecto a los roles y responsabilidades del cargo”]

**Artículo 11. Responsabilidades del oficial de seguridad cibernética y de la información**

[“Establecer procedimientos para el desarrollo del programa de seguridad cibernética y de la información “, “establecer controles para el desarrollo del programa de seguridad cibernética y sus lineamientos”, “monitorear el cumplimiento de los controles para el desarrollo del programa de seguridad cibernética”]

[“Establecer procedimientos para la implementación, control y mantenimiento del programa de seguridad cibernética”, “crear controles para verificar el cumplimiento de los procesos del programa de seguridad cibernética”, “monitorear y realizar un feedback a los controles que sean necesarios para el cumplimiento del programa de seguridad cibernética”]

[“Establecer en el reglamento institucional el desarrollo de políticas, estándares, procedimientos, controles y mantenimientos para el programa de seguridad cibernética”, “Definir en las políticas los objetivos y beneficios para la implementación de nuevos reglamentos, procedimientos y controles”, “Realizar una evaluación de beneficios recibidos por la implementación de políticas, procedimientos y controles “]

[“Establecer una política para el tratamiento de los riesgos”, “crear procedimientos para realizar el tratamiento de riesgos adecuado mediante estándares internacionales”, “crear controles para evaluar el tratamiento establecido a los riesgos de la organización “]

[“Crear una política para establecer los niveles aceptados para la gestión de riesgo”, “crear un procedimiento para la evaluación de los niveles aceptados para el tratamiento del riesgo”, “Establecer un estándar internacional para valorar los niveles de riesgo “]

**Artículo 12. Áreas Especializadas**

[“Establecer una política del perfil del personal para distintas áreas especializadas del comité funcional de seguridad cibernética”, “crear procedimientos para medir el nivel de conocimiento en las áreas especializadas a aplicar por el personal técnico”, “Evaluar las capacidades técnicas, del personal de cada área”]

[“Crear una política que establezca que las entidades de intermediación y participantes del SIPARD deben contar con al menos un área funcional, responsable de la ejecución del programa de seguridad cibernética”, “crear un procedimiento para establecer los pasos para el cumplimiento y ejecución del programa de seguridad cibernética por parte de entidades de intermediación”, “Crear controles para evaluar el cumplimiento y ejecución del programa de seguridad cibernética “]

[“Crear política para establecer que el Oficial de seguridad cibernética es el encargado de nombrar a un profesional encargado de cada área especializada”, “crear procedimiento para verificar el perfil del encargado de cada área especializada “, “Crear controles para evaluar que el encargado de cada área cumpla con los roles y responsabilidades del cargo”]

**TITULO II**

**Artículo 13. Gestión de Riesgos Tecnológicos**

[“Crear una política para realizar análisis de vulnerabilidades periódicamente”, “crear una política para realizar pruebas de penetración por lo menos una vez al año”, “Realizar un análisis de riesgos, para identificar el nivel de seguridad de la organización”]

[“Crear una política para el análisis y evaluación de riesgos tecnológicos como mínimo una vez al año”, “Crear el plan de Análisis y evaluación de riesgos tecnológicos”, “Identificar los activos de la organización, (hardware, software, información, personal, accesorios, etc.)”]

[“Crear una política para el análisis y evaluación de riesgos tecnológicos como mínimo una vez al año”, “Identificar los activos de la organización, (hardware, software, información, personal, accesorios, etc.)”, “Identificar el impacto y la probabilidad de que se materialice una amenaza”]

[“Crear procedimiento para Planificar e implementar el tratamiento de riesgos.”, “Crear un plan de acciones para el tratamiento de riesgo: Eliminar o mitigar riesgo, Asumir riesgo, compartir el riesgo etc.”, “monitoreo y revisión integral del proceso de tratamiento de riesgos”]

[“Crear una política que establezca la revisión integral y el monitoreo de los procesos del tratamiento de riesgos”, “Crear controles para el monitoreo y revisión integral del proceso de tratamiento de riesgos”, “Evaluar la efectividad del tratamiento de riesgos”]

[“Crear un plan de acciones para el tratamiento de riesgo: Eliminar o mitigar riesgo, Asumir riesgo, compartir el riesgo etc.”, “Crear un procedimiento de las medidas o lineamientos que tiene que cumplir el tercero para transferir el riesgo, contratos de confidencialidad entre otros”, “Crear controles para evaluar que la transferencia del riesgo seas tratada adecuadamente por el tercero”]

**Artículo 14. Gestión de Riesgos Tecnológicos en las Entidades Interconectadas**

[“Establecer políticas para que las entidades intermediarias realicen la Gestión de riesgos tecnológicos”, “Establecer controles para verificar el cumplimiento de la entidades intermediarias con la implementación de Gestión de Riesgo”, “Realizar una evaluación de riesgos a entidades intermediarias para determinar objetivamente cuáles son sus riesgos relevantes para la seguridad de su organización”]

[“Establecer controles para verificar el cumplimiento de la entidades intermediarias con la implementación de Gestión de Riesgo”, “Realizar una evaluación de riesgos a entidades intermediarias para determinar objetivamente cuáles son sus riesgos relevantes para la seguridad de su organización”, “monitorear el tratamiento del riesgo a las empresas intermediarias”]

[“Crear una política que establezca sanciones por incumplimiento en la implementación de Gestión de Riesgos a empresas intermediarias”, “Crear políticas para establecer la interconexión a entidades de intermediación financiera cuando sus riesgos sean mayor al definido por el consejo u órgano societario”, “Crear políticas para sancionar preventivamente a entidades de intermediación financiera cuando la evaluación de riesgos a realizar no sea satisfactoria”]

[“Crear políticas para establecer la interconexión a entidades de intermediación financiera cuando sus riesgos sean mayor al definido por el consejo u órgano societario”, “Crear políticas para sancionar preventivamente a entidades de intermediación financiera cuando la evaluación de riesgos a realizar no sea satisfactoria”, “Realizar evaluaciones de Riesgos a entidades de intermediación financiera periódicamente”]

**Artículo 15. Metodologías de la gestión de riesgos tecnológicos.**

**Artículo 35. Comunicaciones Electrónicas**

[“Asignar correo externo a Gerentes”, “Asignar correo electrónico a colaboradores de puestos claves”, “Restringir acceso a correos externos a los colaboradores, salvo a Gerentes, jefes y puestos claves.”]

[“Crear un plan para asignar a los puestos que accederán a la mensajería”, “Asignar a colaboradores de puestos claves el acceso a mensajería instantánea”, “Realizar evaluaciones de cumplimiento”]

[“Crear un plan para determinar los usuarios que tendrán acceso a la plataforma”, “Asignar a los usuarios acceso a portal según políticas de seguridad definidas”, “Realizar evaluaciones de cumplimiento y mejora”]

[“Crear un plan para asignar extensiones a colaboradores que lo necesiten”, “Asignar a colaboradores con puestos claves “, “Realizar un check list y control de las extensiones asignadas para corroborar cumplimiento políticas de seguridad”]

[“Crear un plan y definir políticas para asignar permisos”, “Asignar a los puestos claves los permisos de llamadas claves”, “Realizar un check list y control de las extensiones asignadas para corroborar cumplimiento políticas de seguridad”]

**Artículo 36. Gestión de Proveedores Externos de Producción o Servicios Tecnológicos**

[“Realizar un plan para analizar si es necesario la adquisición de un tercero”, “Establecer los planes que debe cumplir el proveedor por medio de los SLA's”, “Reestablecer los SLA´s (si lo necesitan) para asegurar los servicios “]

[“Crear un plan para documentar y determinar las políticas que se trabajará con el proveedor”, “Corroborar que el proveedor cumpla con los SLA's”, “Reestablecer los SLA´s (si lo necesitan) para asegurar los servicios “]

[“Crear un plan para documentar y determinar las políticas que se trabajará con el proveedor. Estudiar que el proveedor cumpla con un mínimo de 2 normas internacionales”, “Corroborar que el proveedor cumpla con los SLA's”, “Reestablecer los SLA´s (si lo necesitan) para asegurar los servicios “]

[“Crear un plan para documentar y determinar las políticas que se trabajará con el proveedor”, “Analizar a los proveedores por medio de pruebas de calidad para determinar la conveniente”, “Establecer los contratos SLA's y documentarlos”]

[“Establecer manejo de buenas prácticas y determinar ambientes de pruebas”, “Administrar ambientes de pruebas ya que no deben tener mayores privilegios”, “Eliminar los ambientes de pruebas para que el externo lo tenga accesos”]

**37. Gestión de Desarrollo de Sistemas**

[“Establecer política de procesos para segmentar los roles que debe realizar cada colaborador”, “Verificar que las políticas se cumplan”, “Analizar y comprobar de forma anual si las políticas deben ser actualizadas”]

[“Establecer política de procesos para segmentar los roles que debe realizar cada colaborador”, “Verificar que las políticas se cumplan”, “Analizar y comprobar de forma anual si las políticas deben ser actualizadas”]

[“Establecer política de procesos para segmentar los roles que debe realizar cada colaborador”, “Verificar que las políticas se cumplan y documentar los hallazgos”, “Analizar y comprobar de forma anual si las políticas deben ser actualizadas”]

[“Establecer política de procesos para segmentar los roles que debe realizar cada colaborador”, “Verificar que las políticas se cumplan y documentar los hallazgos”, “Analizar y comprobar de forma anual si las políticas deben ser actualizadas”]

[“Establecer políticas de seguridad para determinar el equipo de protección adecuado”, “, “]

**38. Ciclo de Vida del Desarrollo de Sistemas y Aplicaciones**

[“Plan estratégico para la toma de requerimientos”, “Implementación de políticas y metodologías para la toma de requerimientos”, “Capacitar al usuario “]

[“No cuenta con metodologías de ciclo de vida para los sistemas”, “Se cuenta con planes estratégicos para evaluar el ciclo de vida de los sistemas”, “Se establece planes de evaluaciones periódicas para disminuir incidentes”]

[“Establecer y determinar la personalización de los paquetes”, “Implementación de manuales de buenas prácticas”, “Capacitar al usuario “]

[“Establecer planes de Ética Hacking “, “Implementar planes periódicos de ética hacking para determinar nivel de seguridad”, “Mejorar las metodologías, políticas y buenas prácticas”]

[“Establecer planes de seguimiento a los sistemas instalados”, “Evaluar los sistemas para determinar si continúan con los servicios”, “Establecer manejos y planes de incidentes en base a las evaluaciones”]

**Artículo 39. Seguridad Física y del Entorno**

[“Establecer planes estratégicos como BIA”, “Implementar políticas y manuales de seguridad relacionados al BIA”, “Capacitar al usuario y brindar recursos “]

[“Establecer accesos restringidos Colocar equipos de vigilancia Establecer controles de accesos “, “Implementar políticas y controles por medio de equipos de vigilancia y detector de huellas”, “Capacitar al usuario Aplicar control de Accesos “]

[“Establecer rutas de evacuación”, “Colocar mapas de rutas de evaluación Colocar Señalizaciones de las rutas de evaluación”, “Capacitar a los usuarios Aplicar procedimientos de manejos e incidentes”]

[“Establecer evaluación de capacidad para la planta eléctrica”, “Colocar planta eléctrica a centros de datos”, “Realizar mantenimientos a la planta eléctrica”]

[“Realizar planes de inversión para determinar cantidad y capacidad que se aplicará a los centros de datos”, “Colocar los para-rayos en lugares estratégicos”, “Capacitar a los encargados de centros de datos”]

**Artículo 40. Continuidad de las Operaciones Tecnológicas**

[“Establecer planes estratégicos como BIA”, “Aplicar y determinar políticas de seguridad”, “Capacitar al usuario Realizar actualizaciones de los procesos anualmente”]

[“Realizar planes estratégicos y procesos a ejecutar”, “Aplicar los procesos como buena práctica”, “Capacitar al usuario Verificar que los procesos sean cumplidos”]

[“Definir manual de seguridad y estándares donde se regirán”, “Implementar el manual de seguridad”, “Capacitar al usuario “]

[“Definir planes para determinar los roles que debe ejercer cada usuario”, “Implementar los planes estratégicos “, “Capacitar al usuario Notificar a toda la corporación sobre los planes estratégicos”]

[“, “, “]

Artículo 41. Auditorías Internas

[“Realizar planes de implementación para auditorías”, “Definir a cada cuanto tiempo se realizarán esta práctica”, “Capacitar a usuarios para toma de buenas prácticas”]

[“Realizar planes periódicos para auditorías Externas”, “Definir tiempos en que se realizará esta práctica”, “Capacitar a usuarios para toma de buenas prácticas”]

[“Realizar planes de evaluación para determinar los servicios que prestará auditoría”, “Analizar a los auditores por medio de evaluaciones”, “Mantener relación con la auditoría que haya sido mejor calificada”]

[“Establecer planes de auditoría orientadas a la objetividad del negocio”, “Establecer planes de auditoría objetivas y determinar alcances”, “Notificar a alta Gerencia los resultados “]

[“Establecer políticas de estructuración de documentos”, “Implementar el modelo de documentos a presentar”, “Notificar a colaboradores sobre modelo de documento”]

**Artículo 42. Desempeño de la Seguridad**

[“Definir el rol y perfil que debe contar un CEO”, “Contratar al CEO conforme al perfil definido”, “Establecer con CEO los roles y monitoreo de seguridad informática que necesita la corporación”]

[“Establecer normas de buenas prácticas Búsqueda de corporaciones que ofrezcan el servicio”, “Determinar los períodos que realizará “, “Contrato con empresa de servicio”]

[“Establecer informes con CEO para presentarlos Determinar modelos de informes”, “Determinar los períodos que realizará los informes”, “Divulgación de informes para establecer medidas de seguridad”]

[“Determinar planes estratégicos de análisis de sistemas bajo normas internacionales”, “Aplicar las normas establecidas”, “Divulgar información sobre las buenas prácticas de seguridad para ser evaluadas y determinas su madurez”]

[“Determinar formatos de estados de resultados bajo normas Internacionales”, “Aplicar los formatos determinados “, “Divulgar información de cuáles serán los formatos que se utilizarán”]

**Artículo 43. Cumplimiento del monitoreo de la Seguridad**

[“Establecer procesos de seguridad bajo las políticas de seguridad establecidas”, “Corroborar que las políticas sean cumplidas”, “Realizar actualizaciones de políticas de seguridad anualmente”]

[“Establecer roles que ejercerá el hora de seguridad”, “Realizar auditorías para corroborar que el área cumpla con las políticas establecidas”, “El área debe realizar actualizaciones de las políticas de seguridad”]

[“Establecer sanciones conforme el grado de la falta”, “Realizar planes de concientización “, “Monitorear que los colaboradores cumplan con los estándares”]

[“Realizar manuales de seguridad bajo normas Internacionales Determinar procesos definidos para cada control”, “Establecer manuales y políticas de seguridad “, “Capacitar a los Usuarios Divulgar las políticas de seguridad a toda la corporación”]

[“Establecer normas de buenas prácticas para determinar cuándo se actualizarán los manuales”, “Actualizar los manuales conforme a la necesidad de la empresa”, “Actualizar los manuales conforme lo establecido a buenas prácticas, debe estar firmadas y autorizadas por los Gerentes”]

[“, “, “]

**Artículo 44. Estándares Internacionales**

[“Establecer planes de seguridad bajo normas Internacionales y establecer políticas de seguridad”, “Las aplicaciones que se realicen deben cumplir las políticas de seguridad establecidas”, “Realizar actualizaciones de políticas de seguridad anualmente”]

[“, “, “]

[“Establecer políticas de seguridad bajo la norma PA-DSS”, “Corroborar que las políticas sean cumplidas”, “Realizar actualizaciones de políticas de seguridad anualmente”]

[“Establecer políticas de seguridad bajo la norma SWIFT-CSCF”, “Corroborar que las políticas sean cumplidas”, “Actualizar los manuales de seguridad, deben estar apegados a la necesidad de la empresa”]

[“Establecer planes y políticas de seguridad para actualizar los manuales”, “Corroborar que las políticas sean cumplidas”, “Actualizar los manuales y políticas de seguridad”]

**Artículo 45. Estándares**

[“adherirse a el estándar PCI-DSS con la finalidad de manejo seguro de datos para la tarjeta de pagos.”, “crear un programa de gestión de vulnerabilidades o adherir el plan a la CSIRT que exista.”, “actualizar las políticas de seguridad, para mantener los datos a salvo, también se debe actualizar con capacitaciones a los usuarios.”]

[“establecer estrategia de seguridad para el monitoreo y control de acceso, en las áreas.”, “plan de contingencia ante violaciones de seguridad, como el cierre de inmediato activación de protocolos de seguridad.”, “aplicar mejora continua, realizar pruebas de estrés y evaluar el rendimiento”]

[“crear una política de seguridad para la aplicación de métodos de seguridad como tokens, capchat, etc.”, “capacitación y concientización de usuarios.”, “adherirse a nuevas metodologías y controles de inicio de Sesión. Estandarizar estos controles.”]

[“crear una entidad que regule esta acción, o asignarle a el oficial de seguridad.”, “preparar y capacitar a la entidad que regulara.”, “Asignación de roles y responsabilidades.”]

[“, “, “]

**Artículo 46. Informe de Cumplimiento**

[“adherirse a las entidades reguladores para el acceso a las herramientas solicitadas”, “crear un plan que regularice el uso de las herramientas y asignar responsabilidades”, “capacitación constante ante nuevas herramientas digitales”]

**Artículo 47. Requerimientos Adicionales**

[“Diseño de un sistema de alta disponibilidad mediante estándares

como thiers. “, “aplicación del diseño estandarizado, y asegurar la data.”, “mejora de controles, como asegurar la información, back-up, sitios redundantes, mínimo dos enlaces, etc.”]

[“crear un entidad o comité ejecutivo encargado de la capacitación y concientización de uso de las tecnologías de manera adecuada.”, “capacitación de usuarios, sobre el manejo de la información de manera adecuada. “, “implementación de mejora continua y buenas prácticas.”]

**Artículo 48. verificación de entes reguladores y supervisores**

[“adherirse a la entidad reguladora del país.”, “adaptar las metodologías de buenas prácticas que propone los sistemas reguladores.”, “mejora continua”]

[“crear una estrategia de monitoreo y control periódicamente y salvaguardar la información.”, “evaluaciones constantes para verificar el cumplimiento.”, “mejora continua.”]

**TITULO III**

**Artículo 49. Consejo Sectorial**

[“segmentar el consejo según necesidades de la empresa.”, “asignación de responsabilidades

y roles a cada consejo.”, “capacitación constante.”]

[“asignar un miembro con voz y voto en cada consejo.”, “asignación de responsabilidades y roles a cada consejo.”, “capacitación constante.”]

[“elegir el gobernador acorde su experiencia y capacidad de bancos.”, “asignación de responsabilidades y roles a cada consejo.”, “capacitación constante.”]

[“elegir el superintendente de bancos “, “asignación de responsabilidades y roles a cada consejo.”, “capacitación constante.”]

[“elegir el superintendente de valores.”, “asignación de responsabilidades y roles a cada consejo.”, “capacitación constante.”]

[“asignar el controlador de banco “, “asignación de responsabilidades y roles a cada consejo.”, “capacitación constante.”]

[“crear un departamento de control a esta área.”, “asignación de responsabilidades y roles a cada consejo.”, “capacitación constante.”]

[“asignar un presidente que representa en la asociación.”, “asignación de responsabilidades y roles a cada consejo.”, “capacitación constante.”]

[“asignar un presidente de asociaciones de ahorro y préstamos.”, “asignación de responsabilidades y roles a cada consejo.”, “capacitación constante.”]

[“asignar un presidente de asociaciones de ahorro y créditos”, “asignación de responsabilidades y roles a cada consejo.”, “capacitación constante.”]

[“asignar un director para estos incidentes.”, “asignación de responsabilidades y roles a cada consejo.”, “capacitación constante.”]

**Artículo 50. Facultades**

[“crear un plan estratégico para definir los lineamientos de riesgos”, “mejora y revisión constante de nuevas amenazas”, “capacitación constante.”]

[“realizar una evaluación en el marco de actividades y sus funcionamientos”, “aplicar estándares para el manejo de incidentes.”, “capacitación constante.”]

[“crear un consejo para regular la comunicación entres estas entidades”, “crear un plan de coordinación entre las entidades para el manejo de riesgos e incidentes”, “capacitación constante.”]

[“crear un consejo para regular la comunicación entres estas entidades”, “crear un plan de coordinación entre las entidades para el manejo de riesgos e incidentes”, “capacitación constante.”]

[“adherirse a las regulaciones del país.”, “crear una entidad que regule las acciones entorno a las regulaciones del país.”, “capacitación y concientización a los usuarios.”]

[“crear una estrategia para la comunicación segura entre los sectores”, “capacitación a los usuarios.”, “mejora continua a nuevas metodologías de comunicación”]

**Artículo 51. Funcionamiento**

[“crear una política donde se responda a reuniones.”, “adherirse a toda entidad a la política.”, “]

[“, “, “]

**Artículo 52. Creación del mecanismo**

[“crear el presupuesto y modalidades de ejecución de este”, “adherirse a las regulaciones según la junta monetaria. “, “capacitación constante.”]

[“crear el plan y adherirlo a la CSIRT”, “Realizar correcciones y mejora continua ante nuevos incidentes”, “adherir nuevos conocimientos para el plan estratégico a manejo de incidentes”]

**Artículo 53. Responsabilidades**

[“adaptar la acción de la CSRIT a la entidad de la empresa”, “plan estratégico de CONTINUIDAD DEL NEGOCIO Y RECUPERACION”, “buenas prácticas y mejoras continuas mediante capacitación constante.”]

**Artículo 54. Estructura**

[“adherir a una estructura organizada a el CSIRT”, “asignación de responsabilidades a los encargados de control de la CSRIT.”, “capacitación y concientización a los responsables.”]

[“crear una política donde se debe establecer los deberes y responsabilidades”, “asignación de roles y responsabilidades de cada entidad.”, “capacitación y concientización a los responsables.”]

**Artículo 55. Dirección.**

[“asignar a personal que cumpla con los requisitos. “, “capacitación del personal.”, “realizar pruebas y verificar el desempeño adecuado”]

[“asignar a personal que cumpla con los requisitos. “, “capacitación del personal.”, “realizar pruebas y verificar el desempeño adecuado”]

**Artículo 56. Instalaciones**

[“Contactar a los responsables en caso de que CSIRT no tenga un lugar donde operar, tomando como requisito principal: debe ser aislado para poder trabajar y que este principalmente asegurado.”, “Verificar el sitio donde operara CSIRT sea un lugar completamente aislado para que no sea interrumpidas las operaciones y sea seguro.”, “Verificar el sitio donde operara CSIRT se encuentre en óptimas condiciones.”]

[“Contactar a los responsables en caso de que CSIRT no tenga la infraestructura tecnológica que necesita para poder operar y no cuente con los sistemas de información necesarios.”, “Verificar que la infraestructura donde operara CSIRT cumpla con los requisitos necesarios para operar de forma óptima.”, “Verificar que la infraestructura cuente con mantenimiento para un uso óptimo.”]

[“Contactar con el equipo de trabajo en caso de que la información sensible no fue enviada y por tanto no se encuentre almacenada en los sistemas de información.”, “Contactar con el equipo de trabajo en caso de que la información haya sido alterada y se encuentre con errores de lectura.”, “Verificar que la información se encuentre integra y esté disponible en cualquier momento.”]

[“En caso de que el sitio no cuente con un sistema de acceso al sitio de trabajo, deberá adquirir uno para garantizar que el sitio se encuentre seguro.”, “Notificar inmediatamente si el sistema de acceso al sitio de trabajo presenta irregularidades en su funcionamiento.”, “Verificar que la seguridad del sitio de trabajo cuente con mantenimiento para un uso óptimo.”]

[“No realizar ninguna operación en caso de que el consejo sectorial no haya dado aprobado el sitio de trabajo para su uso.”, “Realizar los trámites necesarios para que el consejo sectorial apruebe el sitio de trabajo.”, “Mantener el centro de datos en óptimas condiciones.”]

[“Notificar inmediatamente a los responsables, en caso de encontrar el equipo fuera de las instalaciones de CSRT y posteriormente verificar que los equipos no presenten anormalidades en su uso.”, “Informar inmediatamente en caso de que los equipos no estén funcionando correctamente, dentro de las instalaciones de CSRT.”, “Mantener un control sobre los equipos que se encuentren dentro de las instalaciones del CSRT.”]

**Artículo 57. Definición de Políticas**

[“Informar inmediatamente sobre el personal que este incumpliendo con los lineamientos establecidos, en caso de que sea algo recurrente solicitar personal nuevo que cumpla con lo establecido.”, “Mantener al día al personal sobre cualquier cambio en los lineamientos.”, “Ofrecer capacitaciones continuas sobre el acuerdo sectorial.”]

[“Informar a los responsables sobre la inexistencia o del incumplimiento de las políticas.”, “Dar capacitaciones sobre las políticas de la organización.”, “Tener un control sobre el cumplimiento de las políticas actualizado.”]

**Artículo 58. Establecimiento de los Servicios**

[“Notificar a los responsables sobre la inexistencia de los servicios establecidos por la CSIRT.”, “Validar que el servicio establecido de seguridad cibernética haya sido implementado dentro del CSIRT.”, “Monitorear el servicio establecido.”]

[“Notificar a los responsables en caso de ayuda inexistente sobre los incidentes ocurridos.”, “Validar el cumplimiento de los procesos.”, “Tener un historial sobre el número de veces que las entidades financieras recibieron apoyo.”]

**TITULO IV**

**Artículo 59. Sanciones.**

[“Informar sobre la inexistencia de un reglamento de sanciones.”, “Existen sanciones definidas en el reglamento, pero no se están aplicando correctamente.”, “Monitorear la aplicación de la sanción.”]

[“Informar el incumplimiento de los instructivos en las áreas correspondientes.”, “Existen los instructivos, pero no se aplican correctamente.”, “Monitorear la aplicación de los instructivos a las entidades monetaria y financiera.”]

**Articulo 60 Medidas Precautorias**

[“Informar sobre el incumplimiento de sanciones.”, “No se están aplicando correctamente las sanciones para el interconexión o intercambio de información.”, “Monitorear el apoyo y servicios conexos.”]

[“Incumplimiento sobre de la suspensión de los miembros de los miembros del SIPARD.”, “No se aplican de forma apropiada las sanciones.”, “Monitorear a los miembros del SIPARD que hayan sido.”]

[“, “, “]

**Artículo 61. Elaboración de Instructivos y Circulares**

[“Informar inmediatamente sobre la inexistencia de instructivos para la prueba.”, “Los instructivos no se aplican de forma adecuada para la prueba.”, “Monitorear las cantidades de insumos necesarios.”]

[“Informar sobre el descontrol de versionamiento de los reglamentos, o inexistencias de los mismos.”, “Los reglamentos se encuentran actualizados, pero no están autorizados.”, “Tener un control de versiones al día por cada reglamento creado.”]

**Artículo 62. Plazo de Adecuación**

[“Notificar a las autoridades en caso de que las entidades no se encuentren ajustadas al reglamento y no cuente con el mínimo establecido.”, “Las entidades no cuentan con el tiempo mínimo establecido y se encuentran ajustadas al reglamento.”, “Monitorear el cumplimento del reglamento.”]

[“, “, “]