ANEXO N°1

MATERIAS MÍNIMAS PARA CONSIDERAR EN LOS ANÁLISIS DE RIESGOS DE CIBERSEGURIDAD

Controles organizacionales

• Políticas de seguridad de la información
• Roles y responsabilidades de seguridad de la información
• Segregación de deberes
• Responsabilidades de gestión
• Contacto con autoridades
• Contacto con grupos de interés especial
• Inteligencia de amenazas
• Seguridad de la información en la gestión de proyectos
•Inventario de información y otros activos asociados
• Uso aceptable de información y otros activos asociados.
• Retorno de activos
• Clasificación de la información
• Etiquetado de información
• Transferencia de información
• Control de acceso
• Gestión de identidad
• Información de autenticación
• Derechos de acceso
• Seguridad de la información en las relaciones con los proveedores
• Abordar la seguridad de la información dentro de los acuerdos con proveedores
• Gestión de la seguridad de la información en la cadena de suministro de las TIC
• Seguimiento, revisión y gestión de cambios de los servicios de proveedores.
• Seguridad de la información para el uso de servicios en la nube
• Planificación y preparación de la gestión de incidentes de seguridad de la información
• Evaluación y decisión sobre eventos de seguridad de la información
• Respuesta a incidentes de seguridad de la información
• Aprendiendo de los incidentes de seguridad de la información
• Recolección de evidencia
• Seguridad de la información durante la interrupción
• Preparación de las TIC para la continuidad empresarial
• Identificación de requisitos legales, estatutarios, regulatorios y contractuales
• Derechos de propiedad intelectual
• Protección de registros
• Privacidad y protección de datos personales o sensibles
• Revisión independiente de la seguridad de la información
• Cumplimiento de políticas y estándares de seguridad de la información
• Procedimientos operativos documentados

Controles de personas

• Verificación de personal respecto de sus capacidades y habilidades para los roles asignados
• Términos y condiciones de empleo
• Sensibilización, educación y formación en seguridad de la información
• Proceso Disciplinario
• Responsabilidades después de la terminación o cambio de empleo

• Acuerdos de confidencialidad o no divulgación
• Trabajo remoto
• Informes de eventos de seguridad de la información

Controles físicos
• Perímetro de seguridad física
• Controles de entrada física
• Asegurar oficinas, salas e instalaciones
• Monitoreo de seguridad física
• Protección contra amenazas físicas y ambientales
• Trabajando en áreas seguras
• Escritorio despejado y pantalla despejada
• Ubicación y protección de equipos
• Seguridad de los activos fuera de las instalaciones
• Medios de almacenamiento
• Utilidades de apoyo
• Seguridad del cableado
• Mantenimiento de equipo
• Eliminación o reutilización segura de equipos

Controles tecnológicos
• Dispositivos endpoint de usuario
• Derechos de acceso privilegiado
• Restricción de acceso a la información
• Acceso al código fuente
• Autenticación segura
• Gestión de capacidad
• Protección contra malware
• Gestión de vulnerabilidades técnicas
• Gestión de la configuración
• Eliminación de información
• Enmascaramiento de datos
• Prevención de fuga de datos
• Respaldo de información
• Redundancia de instalaciones de procesamiento de información
• Inicio sesión
• Actividades de seguimiento
• Sincronización de reloj
• Uso de programas de utilidad privilegiados
• Instalación de software en sistemas operativos
• Controles de red
• Seguridad de los servicios de red
• Filtrado web
• Segregación en redes
• Uso de criptografía
• Ciclo de vida de desarrollo seguro
• Requisitos de seguridad de la aplicación
• Principios de ingeniería y arquitectura de sistemas seguros
• Codificación segura
• Pruebas de seguridad en desarrollo y aceptación
• Desarrollo subcontratado

- Separación de entornos de desarrollo, prueba y producción
- Gestión del cambio
- Información de prueba
- Protección de los sistemas de información durante la auditoría y las pruebas.