PROPUESTA

CONSULTORÍA EN LA IMPLEMENTACIÓN DE UN MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN CORPOCALDAS

GERENCIA@ZSEGURIDAD.COM.CO

PROYECTOS@ZSEGURIDAD.COM.CO

313 749 88 42 - 311 621 79 33

CRA. 23A N° 74 – 238, MANIZALES - CALDAS

CORPOCALDAS
RUBEN DARIO JARAMILLO
DIRECTOR DE TI
MANIZALES, 18 DE febrero DE 2023

Señor Rubén Darío:

Después de conversar sobre las necesidades puntuales que tiene la entidad con respecto a la seguridad de la información, ponemos en consideración la siguiente propuesta para el **Diagnóstico e Implementación del Modelo de Gestión de Seguridad y Privacidad de la Información**, velando por el cumplimiento de la normatividad vigente y generar valor público.

Ponemos a su consideración la experiencia de todo un equipo de consultores en organizaciones privadas y públicas, que permiten, con criterio técnico especializado, poder aportarle a su gestión de una manera efectiva.

Todo nuestro equipo altamente calificado se encontrará a su disposición para cualquier inquietud y/o sugerencias.

Atentamente,

Paola Tatiana Mesa Dávila
Consultora en Seguridad Informática

PROPUESTA

CONSULTORÍA EN LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN CORPOCALDAS

OBJETIVOS DE ESTA PROPUESTA

- Realizar un diagnóstico que permita identificar el nivel de madurez actual de la organización basado en el modelo de seguridad y privacidad de la información de MINTIC.
- Brindar consultoría especializada para la implementación por fases del Modelo de Seguridad y Privacidad de la Información, de acuerdo con las buenas prácticas establecidas por MINTIC.
- Brindar una capacitación especializada en seguridad digital a los usuarios de la corporación. Aplicando la metodologías de concientización en ciberseguridad y seguridad digital

EQUIPO PRINCIPAL DE TRABAJO

CONSULTOR SEMI SENIOR EN SEGURIDAD DE LA INFORMACIÓN Y AUDITOR DE SISTEMAS

- Ingeniera de Sistemas y Telecomunicaciones.
- Máster en Tecnologías Informáticas Avanzadas.
- Máster en Tecnologías Web
- Especialista en Redes y Comunicaciones
- Auditor interno
- **Certificada como Auditora ISO 27001**
- **Certificada como Auditora ISO 22301**
- **Certificada en Ciberseguridad CSX de ISACA.**
- 8 años de experiencia como consultora implementando Modelos de Seguridad y Ciberseguridad.

CONSULTOR EN GERENCIA ESTRATEGICA DE SISTEMAS Y MODELOS DE SEGURIDAD INFORMATICA. GERENTE PROYECTO

- Asesor y Consultor en Modelos de Seguridad Informática, Tecnologías de la Información y Comunicación y Sistemas de Información Gerenciales (ERP-CRM).
- Consultor en Gerencia de Proyectos e Implementaciones de Proyectos de TI.
- Administrador de Sistemas Informáticos –UNAL
- Magister en Administración de Empresa –UNAL
- Certificado Project Management Professional (PMP)®
- 8+ años de experiencia como CIO, con múltiples implementaciones y dirección de proyectos tecnológicos, tanto privados como públicos.
- Experiencia en Gestión de la Seguridad Informática y en Auditoría de Sistemas.

CONSULTOR JUNIOR EN SEGURIDAD DE LA INFORMACIÓN

- Administradora pública
- Auditor interno en sistemas de gestión de seguridad de la información NTC ISO/IEC 27001:2013
- Auditor interno en sistemas de calidad NTC ISO 9001:2015
- Oficial de privacidad / Protección de datos personales 2018
- Formación integral para los jefes de control interno, MIPG
- Gestión de proyectos con base en PMI
- 2 años de experiencia como consultora

NOTA: ***Es necesario la participación de uno o varios representantes de Corpocaldas según lo requiera el plan del proyecto que facilite la recolección de la información necesaria para el desarrollo de este. Así mismo Zeta Seguridad de la Información pondrá a disposición de Corpocaldas una persona documentadora medio tiempo en sitio durante toda la semana.***

ACTIVIDADES Y ENTREGABLES PRINCIPALES

FASE	Descripción	Entregable	Tiempo / Semanas
FASE 1 **DIAGNÓSTICO**	Identificar el nivel de madurez de seguridad y privacidad de la información en que se encuentra la entidad, como punto de partida para la implementación del MSPI.	Informe resultado de autodiagnóstico y acciones de mejora.	6
	Identificar las vulnerabilidades en Red LAN y Perímetro (firewall)	Informe resultado vulnerabilidades de Red LAN y Perimetral	
	Conocer en detalle las características de la entidad y su entorno, permitiendo adaptar el MSPI de acuerdo con las condiciones especificas de la entidad.	Matriz DOFA del MSPI. Contexto de la entidad desde el plan estratégico empresarial.	
	Conocer las expectativas que se tiene respecto a la implementación del MSPI para garantizar su cumplimiento.	Partes interesadas desde el plan estratégico empresarial.	
	Identificar que información será protegida mediante la adopción del MSPI.	Alcance del MSPI.	
	Garantizar el liderazgo y el compromiso para conseguir los objetivos definidos para la implementación del MSPI.	Gestionar dicho liderazgo por parte de la empresa. Evidenciar dicha gestión.	
	Orientar y apoyar por parte de la alta dirección de la entidad la	Política de seguridad y privacidad de la información.	

FASE 2 **PLANIFICACIÓN**	gestión de la seguridad de la información de acuerdo con la misión, normatividad y reglamentación pertinente.	Manual de políticas de seguridad de la información.	16
	Asegurar que los funcionarios de la entidad conozcan qué se espera de ellos, cuál es su impacto en la seguridad de la información y de que manera contribuyen con la adopción del MSPI.	Documento de roles y responsabilidades asociados a la seguridad y privacidad de la información.	
	Estructurar una metodología que permita identificar y clasificar los activos de información.	Procedimiento con metodología de inventario y clasificación de la información. Inventario de activos de información actualizado de acuerdo con la metodología definida en clasificación de activos de información.	
	Estructurar una metodología que permita gestionar los riesgos de seguridad y privacidad de la información.	Procedimiento y metodología de gestión de riesgos. Matriz de riesgos en seguridad de la información.	
	Garantizar una correcta comunicación, sensibilización y concientización con respecto a la seguridad y privacidad de la información, en la que todos los funcionarios conozcan las políticas y su rol en el cumplimiento del MSPI.	Plan de capacitación y sensibilización. Plan de comunicación del MSPI.	
	Implementar los planes y controles para lograr los objetivos del MSPI.	Plan de implementación de controles de seguridad y privacidad de la información. Evidencia de implementación de los controles de seguridad y privacidad de la información.	

FASE 3 **OPERACIÓN**			4
	Identificar el nivel de madurez de seguridad y privacidad de la información actual en la entidad, después de implementar la fase 1 y fase 2.	Informe de nivel de madurez del MSPI	
	Evaluar el desempeño de seguridad de la información y la eficacia del MSPI.	Hoja de vida de indicadores. Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos.	
FASE 4 **EVALUACIÓN DE DESEMPEÑO**	Acompañar una auditoría interna para identificar hallazgos del MSPI	Procedimiento medidas correctivas. Plan de auditorías aprobado.	4
	Revisar el MSPI de la entidad, por parte de la alta dirección, en los intervalos planificados, que permita determinar su conveniencia y eficacia.	Revisión a la implementación. Acta de revisión por la dirección. Compromisos de la revisión por la dirección.	
FASE 5 **MEJORAMIENTO CONTINUO**	Identificar las acciones asociadas a la mejora continua del MSPI y de los procesos	Plan anual de mejora del MSPI.	2
FASE 6 **SENSIBILIZACIÓN CIBERSEGURIDAD**	Aplicación de estrategias y modelos de capacitación y concientización en ciberseguridad y seguridad digital	. Informe Diagnóstico . Charlas, talleres, webinars, campañas por correo para crear consciencia . Entrenamiento, conocimiento avanzado, prácticas, seguimiento y certificación. . Seguridad ofensiva, Phising, smishing, vishing, clonación, wireless attacks e ingeniería social. . Iteración, nuevas formas de a ataque y defensa.	48

HOJA DE RUTA INICIAL (Puede cambiar según lo encontrado en el análisis inicial)

FASE	Descripción	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
FASE 1 DIAGNÓSTICO	Identificar el nivel de madurez de seguridad y privacidad de la información en que se encuentra la entidad, como punto de partida para la implementación del MSPI.	■	■	■	■																								
	Realizar análisis de vulnerabilidades en Red LAN y Perímetro (Firewall)		■	■																									
	Conocer en detalle las características de la entidad y su entorno, permitiendo adaptar el MSPI de acuerdo con las condiciones especificas de la entidad.		■	■																									
	Conocer las expectativas que se tiene respecto a la implementación del MSPI para garantizar su cumplimiento.			■	■																								
	Identificar que información será protegida mediante la adopción del MSPI.				■																								
	Garantizar el liderazgo y el compromiso para conseguir los objetivos definidos para la implementación del MSPI.					■	■																						
FASE 2 PLANIFICACIÓN	Orientar y apoyar por parte de la alta dirección de la entidad la gestión de la seguridad de la información de acuerdo con la misión, normatividad y reglamentación pertinente.					■	■	■	■	■	■	■	■	■	■														
	Asegurar que los funcionarios de la entidad conozcan qué se espera de ellos, cuál es su impacto en la seguridad de la información y de que manera contribuyen con la adopción del MSPI.					■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
	Estructurar una metodología que permita identificar y clasificar los activos de información.					■	■	■	■																				
	Estructurar una metodología que permita gestionar los riesgos de seguridad y privacidad de la información.							■	■	■	■	■	■																
	Garantizar una correcta comunicación, sensibilización y concientización con respecto a la seguridad y privacidad de la información, en la que todos los funcionarios conozcan las políticas y su rol en el cumplimiento del MSPI.					■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
FASE 3 OPERACIÓN	Implementar los planes y controles para lograr los objetivos del MSPI.										■	■	■	■	■	■	■	■	■										
	Identificar el nivel de madurez de seguridad y privacidad de la información actual en la entidad, después de implementar la fase 1 y fase 2.										■	■	■	■	■	■	■	■	■										
	Evaluar el desempeño de seguridad de la información y la eficacia del MSPI.										■	■	■	■	■	■	■	■	■										
FASE 4 EVALUACIÓN DE DESEMPEÑO	Realizar auditorías internas e identificar hallazgos del MSPI															■	■	■	■	■	■	■	■						
	Revisar el MSPI de la entidad, por parte de la alta dirección, en los intervalos planificados, que permita determinar su conveniencia y eficacia.															■	■	■	■	■	■	■	■						
FASE 5 MEJORAMIENTO CONTINUO	Identificar las acciones asociadas a la mejora continua del MSPI y de los procesos																							■	■	■	■		
FASE 6 SENSIBILIZACIÓN CIBERSEGURIDAD	Actividades de concientización y capacitación en seguridad de la información	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

PROPUESTA ECONÓMICA

SERVICIO/PRODUCTO	INVERSIÓN
FASE 1: DIAGNÓSTICO EN SEGURIDAD DE LA INFORMACIÓN	***$ 25.000.000***
ANÁLISIS DE VULNERABILIDADES EN RED LAN Y PERIMETRAL (20 HORAS)	***$ 5.400.000***
FASE 2: PLANEACIÓN	***$ 32.000.000***
FASE 3: OPERACIÓN	***$ 32.000.000***
FASE 4 y 5: EVALUACIÓN DE DESEMPEÑO Y MEJORAMIENTO CONTINUO	***$ 32.000.000***
FASE 6: SENSIBILIZACIÓN EN CIBERSEGURIDAD - Diagnóstico en ciberseguridad para 300 usuarios - Paquete de 6 charlas de 1 hora en ciberseguridad, se dictará una charla por mes.	***$ 25.000.000***
TOTAL PROYECTO DE GESTION DE SEGURIDAD DE LA INFORMACIÓN	***$ 151.400.000***

IVA incluido

La propuesta es válida para CORPOCALDAS y se podrían contratar por fases.

Por ser una empresa de Manizales, los gastos de viáticos, transporte y alimentación serán asumidos por **ZETA Seguridad de la Información.**

ACUERDOS DEL SERVICIO

ZETA Seguridad de la Información, estará disponible de lunes a viernes de 8:00am a 12:00am y de 1:00 pm a 5:00pm, para cualquier soporte, reunión o consulta requerida por parte de **Corpocaldas.**

FORMA DE PAGO

Se realizarán pagos mensuales de acuerdo con las fases contratadas.

VALIDEZ DE LA PROPUESTA

La presente propuesta será válida durante 30 días, a partir de la fecha.

SUPUESTOS, RESTRICCIONES Y CONSIDERACIONES ADICIONALES

- No se incluye certificación de Modelos de Seguridad.
- Para el desarrollo de la labor encomendada se requiere el apoyo y compromiso por parte de **Corpocaldas**, para cumplir con las fechas establecidas y la calidad esperada.
- Se contará con una persona dedicada al proyecto que tenga el perfil necesario para apoyar todos los procesos documentales que requiera dicha implementación, por lo cual se contará con trabajo semi presencial, se desarrollarán las funciones desde equipos propios. Si son requeridas reuniones de carácter presencial, se agendarán con la debida anterioridad por las partes.
- Se está dispuesto para atender las observaciones e inquietudes que surjan luego de la revisión de la propuesta, y realizar ajustes de acuerdo con lo acordado, en todo caso, estos cambios deberán quedar por escrito, a través de correo electrónico o de acuerdo las políticas y normatividad de **Corpocaldas.**
- El lugar y la logística para las capacitaciones deberá ser suministrado por **Corpocaldas**.

CONFIDENCIALIDAD

ZETA Seguridad de la Información, se compromete al manejo confidencial de la información recibida de manera directa o indirecta, en forma verbal, escrita, gráfica, en medio magnético o bajo cualquier otra forma, de acuerdo a las indicaciones de **Corpocaldas** se compromete al manejo de la

información suministrada exclusivamente para desarrollar las tareas que deriven directamente del cumplimiento del proyecto.

Se considera de carácter confidencial la información suministrada en esta propuesta comercial, por lo tanto, deberá evitarse que sea accesible a las organizaciones o personas que no estén relacionadas con el proceso para el cual fue solicitado. Este documento se considera propiedad intelectual de **ZETA Seguridad de la Información**.

NUESTROS SERVICIOS

- Análisis Inicial de Diagnóstico de Seguridad de la Información.
- Asesoría e Implementación de Sistemas de Gestión en Seguridad de la Información.
- Consultoría para Certificación ISO 27001.
- Análisis y Gestión de Vulnerabilidades. - Hacking Ético
- Análisis y Gestión de Riesgos de Seguridad.
- Consultoría en Protección de Datos Personales - Habeas Data (Ley 1581).
- Asesoría y Consultoría Gestión Estratégica de Tecnología.
- Capacitación y Concientización en Seguridad de la Información.
- Webinars y Conferencias sobre Seguridad de la Información.

CLIENTES Y EXPERIENCIACLIENTES Y EXPERIENCIA

Algunos de nuestros clientes, en diferentes servicios:





















