Digital User
Ciberseguridad para todos

Pereira, 20 de febrero de 2023

Ingeniero
RUBÉN DARÍO JARAMILLO
Director TI
CORPORACIÓN AUTÓNOMA DE CALDAS / CORPOCALDAS
E.S.D

ASUNTO: Propuesta Asesoría en el diagnóstico e implementación del Modelo de Seguridad .

Apreciados señores

Digital User es una empresa especializada en el área de Ciberseguridad, abarcando las capas de seguridad informática EndPoint y Perímetro con tecnología de punta como lo es SOPHOS Antivirus, Sophos XG Firewall y Palo Alto Networks Firewall, en capa Usuario final contamos con un gran portafolio de servicios en capacitación y entrenamiento a usuarios digitales en materia de seguridad digital; permitiendo diagnosticar, desarrollar y fortalecer un coeficiente de detección de amenazas que les permita proteger sus datos personales y corporativos de los ciberdelincuentes. Esto nos convierte en la compañía pionera en Colombia en la comercialización de productos y servicios dirigidos no solo a la capa EndPoint y Perímetro sino también lograr cubrir una capa tan importante como lo es la capa de usuarios finales, propiciando el fortalecimiento de habilidades empresariales para la transformación digital de forma segura.

Contamos en nuestra área de TI con un líder que suma más de 10 años de experiencia en seguridad informática ofensiva (ethical hacking) y defensiva (cloud, perímetro y EndPoint) lo que nos permite tener una visión global y precisa de los mecanismos de ataque utilizados por los ciberdelincuentes, pieza clave en el desarrollo de estrategias para poder implementar de manera efectiva toda la seguridad informática de su compañía.

Entre sus aliados estratégicos están los clústers reconocidos como el ***Nodo Tic*** en la estrategia de la red de Innovación, Ciencia y Tecnología del departamento de Risaralda y el clúster ***NOVITAS***, con el cual hemos iniciado una campaña de sensibilización a empresarios del departamento de Risaralda a través de diferentes actores de la industria TI.
Con gusto estaré dispuesta a resolver cualquier inquietud

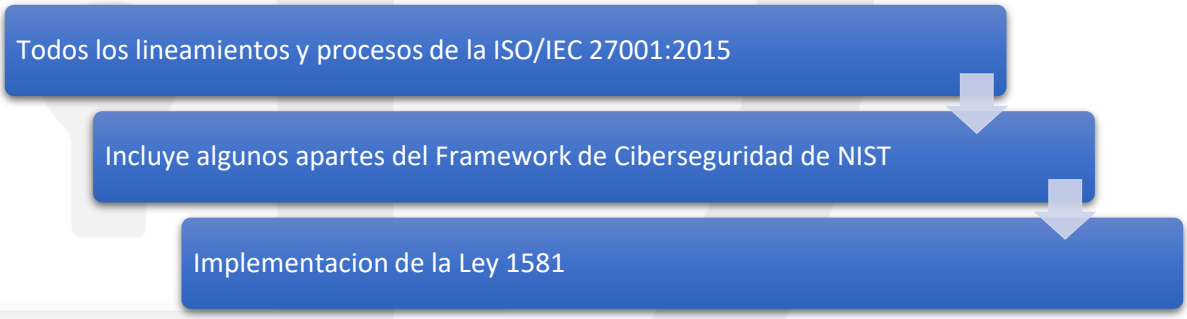
María Fernanda Arcila
Gerente General

OBJETIVO

Asesoría en el diagnóstico e implementación del Modelo de Seguridad

ANTECEDENTES

- *Decreto 1499 de 2017,* sugiere la creación y el cumplimiento de las políticas de Gestión y Desempeño Institucional y comprenderán, entre otras: El Gobierno Digital
- El Gobierno Digital hace parte del MIPG. Y a través del MANUAL DE GOBIERNO DIGITAL se dan los lineamientos para la Implementación de la Política de Gobierno Digital (Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2))
- Las entidades públicas a las que les aplica el Modelo Integrado de Planeación y Gestión – MIPG, deben diagnosticar e implementar los componentes de GOBIERNO DIGITAL y la implementación del Modelo de Seguridad y Privacidad de la Información MSPI y entender de buena manera en que nivel están en la aplicación de las estrategias estipuladas por el MinTIC.
- Según la Resolución 500 de 2021 las entidades públicas deben implementar todo lo concerniente a la Seguridad Digital su CONPES, y ya tener un MSPI en un estado muy maduro.
- En resumen, el MSPI contiene y requiere aplicar:



La implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la entidad, con el objetivo de preservar la confidencialidad,

integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos. (Manual de Gobierno Digital)

PROPUESTA

Diagnosticar e implementar del Modelo de Seguridad y Privacidad de la Información en Corpocaldas

ENTREGABLES

FASE	DESCRIPCIÓN	ENTREGABLES	TIEMPO
Diagnóstico	Permite establecer el estado actual de la implementación de la seguridad y privacidad de la información, para tal fin se debe realizar un "Diagnóstico" utilizando el "instrumento de evaluación MSPI" con el que se identifica de forma específica los controles implementados y faltantes y así tener insumos fundamentales para la fase de planificación	Documento con el resultado de la herramienta de autodiagnóstico, identificando la brecha en la implementación del MSPI en toda la Entidad, y sus acciones de mejora. Plan de Implementación del Modelo de Seguridad y Privacidad de la Información	1 MES
Planificación	Para el desarrollo de esta fase se debe utilizar los resultados de la fase anterior y proceder a elaborar el Plan de Seguridad y Privacidad de la Información con el objetivo de que la Entidad realice la planeación del tiempo, recursos y presupuesto de las actividades que va a desarrollar relacionadas con el MSPI.	Matriz DOFA del Modelo de Seguridad y Privacidad de la Información Contexto de la entidad desde el Plan Estratégico Empresarial Partes interesadas desde el Plan Estratégico Empresarial Alcance del MSPI Evidencia en el acto administrativo que soporta la conformación del comité de gestión y desempeño o quien haga sus veces, señalando las funciones de seguridad y privacidad de la información. Manual de Políticas de Seguridad de la Información	2 MESES

		Política de Seguridad y Privacidad de la Información con Acto administrativo con la adopción de esta	
		Procedimientos de Seguridad de la Información	
		Documento de roles y responsabilidades asociadas a la seguridad y privacidad de la información	
		Inventario de Activos de Información	
		Procedimiento con metodología de inventario y clasificación de la información	
		Inventario de Activos de Información actualizado de acuerdo a la metodología definida de clasificación de activos de información.	
		Procedimiento y metodología de gestión de riesgos institucional incluyendo el capítulo de seguridad y privacidad de la información aprobado por el comité de coordinación de control interno	2 MESES
		Matriz de Riesgos en Seguridad de la Información	
		Declaración de aplicabilidad, aceptada y aprobadas en el comité de gestión institucional.	
		Plan de tratamiento de riesgos, aprobado por los dueños de los riesgos y el comité institucional de gestión y desempeño (Decreto 612 de 2018 Publicación antes de 31 de enero de cada vigencia).	
		Incluir dentro de los proyectos de inversión de la Entidad aquellas actividades relacionadas con la adopción de MSPI de acuerdo con el alcance establecido (Plan de recursos destinados a MSPI	
		Plan de cambio, cultura, apropiación, capacitación y sensibilización de Seguridad y Privacidad de la Información y seguridad digital.	

		Plan de comunicaciones del modelo de seguridad y privacidad de la información.	
Operación	Una vez culminada las actividades del MSPI de la fase de Planificación, se llevará acabo la implementación de los controles, con el fin de dar cumplimiento con los requisitos del MSPI. Los documentos generados generar en esta fase son: ▪ Plan de implementación de controles de seguridad y privacidad de la información ▪ Evidencia de la implementación de los controles de seguridad y privacidad de la información	Plan de implementación de controles de seguridad y privacidad de la información	1 MES
		Evidencia de la implementación de los controles de seguridad y privacidad de la información	
		Informe del Nivel de madurez del Modelo de Seguridad y Privacidad de la Información	
Evaluación de Desempeño	Una vez culminada las actividades del MSPI, se evalúa la efectividad de las acciones tomadas a través de los indicadores definidos en la fase de implementación que debe incluir la correcta interacción entre el MSPI, MIPG y los requerimientos de la Ley 1581 de 2012 “Protección de datos personales”, Ley 1712 de 2014 “Ley de Transparencia y Acceso a la Información Pública”, Decreto 2106 de 2019 o cualquier norma que las reglamente, adicione, modifique o derogue.	Hoja de vida de indicadores, los cuales deben incluirse en el tablero de control del plan de acción, tal como lo ordena el decreto 612 de 2018.	1 MES
		Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos	
		Resultados de las auditorías internas	
		No conformidades de las auditorías internas.	
		Plan de auditorías que evidencia la programación de las auditorias de seguridad y privacidad de la información	
		Procedimiento medidas correctivas	
		Revisión a la implementación	
		Acta y documento de Revisión por la Dirección.	
		Compromisos de la Revisión por la Dirección	

Mejoramiento Continuo	Una vez culminada las actividades del MSPI de la fase evaluación y desempeño, se consolidan los resultados obtenidos de la fase de evaluación de desempeño y diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas	Plan anual de mejora del MSPI	1 MES
CONCIENTIZACIÓN USUARIOS FINALES	Aplicación de estrategias y modelos de capacitación y concientización en ciberseguridad y seguridad digital según guía 14 del MSPI	- Diagnóstico inicial con plan de acción - Charlas para creación de conciencia. - Entrenamiento, conocimiento avanzado, prácticas, seguimiento y certificación. - Seguridad ofensiva, Phishing.	7 MESES

1. DIAGNOSTICO E IMPLEMENTACION DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PROBLEMÁTICA

El Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, es consecuente con la realidad de que las entidades públicas están cada vez más expuestas a sufrir incidentes de seguridad digital, por lo que puede afectar su funcionamiento repercutiendo en la prestación de los servicios a la ciudadanía. Razón por la cual, el ministerio como entidad encargada de diseñar, adoptar y promover políticas, planes, programas y proyectos en el uso y apropiación de las TIC, así mismo, establece lineamientos con el objetivo de generar confianza en el uso del entorno digital, garantizando el máximo aprovechamiento de las tecnologías de la información y las comunicaciones. La política de gobierno digital tiene como objetivo promover lineamientos, planes, programas y proyectos en el uso y apropiación de las TIC para generar confianza en el uso del entorno digital, propendiendo el máximo aprovechamiento de las tecnologías de la información y las comunicaciones.

Teniendo en cuenta lo anterior, el MinTIC elaboró el Modelo de Seguridad y Privacidad de la Información – MSPI y define los lineamientos para la implementación de la estrategia de

seguridad digital, con el objetivo de formalizar al interior de las entidades un sistema de gestión de seguridad de la información – SGSI y seguridad digital, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento.

Adicional, La Resolución 500 de 2021 las entidades públicas deben implementar todo lo concerniente a la Seguridad Digital su CONPES, y ya tener un MSPI en un estado muy maduro.

OBJETIVO

- Diagnosticar e implementar el Modelo de Seguridad y Privacidad de la información en Corpocaldas. Incluyendo lineamientos y procesos de la ISO/IEC 27001:2015, framework de ciberseguridad, y revisión ley 1581 protección de datos.

PLAN DE ACCION

1. Diagnóstico: Realizar diagnóstico o un análisis GAP, cuyo objetivo es identificar el estado actual de la entidad respecto a la adopción del MSPI. Se requiere apoyo de la entidad.

2. Planificación: Determinar las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo.

3. Operación: Se realizará un acompañamiento para la implementación de los procesos y procedimientos del modelo MSPI así como las recomendaciones para la implementación de los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.

4. Evaluación de desempeño: Acompañar a la entidad para determinar de qué manera va a ser evaluado la adopción del modelo. Realizar una Auditoria Interna básica para evaluar cómo se implementó.

5. Mejoramiento Continuo: Se deben establecer procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición. Cada una de las fases se dará por completada, cuando se cumplan todos los requisitos definidos en cada una de ellas.

Digital User
Ciberseguridad para todos

CAPACITACIÓN ESPECIALIZADA A USUARIOS FINALES DE CORPOCALDAS

PROBLEMÁTICA

Una de las grandes problemáticas que enfrenta el gobierno colombiano según su CONPES 3995 de 2020 es; "La creciente participación de ciudadanos en el entorno digital, la alta dependencia de la infraestructura digital y el aumento en el uso y adopción de nuevas Tecnologías de la Información y las Comunicaciones (TIC) trayendo consigo una serie de riesgos e incertidumbres relacionados con la seguridad digital, lo cual exige que el país cuente con suficientes capacidades para su gestión adecuada y oportuna. Las amenazas, los ataques e incidentes de seguridad digital cada día son más sofisticados y complejos e implican graves consecuencias de tipo económico o social. Por ejemplo, según estimaciones de Accenture, el costo para los negocios derivado del impacto de los ciberdelitos ha incrementado en un 72% entre 2014 y 2019 (Accenture, 2019). Esto conlleva al deterioro de la confianza digital y la desaceleración del desarrollo de los países en el futuro digital3. Debido a lo anterior, los gobiernos alrededor del mundo han venido atendiendo los nuevos retos para la detección y manejo de amenazas, ataques e incidentes cibernéticos mediante la formulación y actualización de estrategias o políticas relacionadas con la seguridad digital".

OBJETIVO

Identificar los activos intangibles críticos mediante el software ESLABON CDA en la capa usuario final y así fortalecer las capacidades en seguridad digital de los colaboradores de Corpocaldas con la Metodología MECCI, para así mitigar el riesgo de sufrir un ataque informático dentro de la corporación.

PLAN DE ACCIÓN

METODOLOGÍA DE CONCIENTIZACIÓN EN CIBERSEGURIDAD (MECCI)



FASE 1 – DIAGNÓSTICO EN CIBERSEGURIDAD

El diagnóstico permite medir rápidamente el nivel de riesgo al que está expuesto su compañía de sufrir un ataque informático producto de la ausencia de un programa de entrenamiento a sus usuarios; permitiéndole con las estadísticas obtenidas realizar un plan de acción contundente y a la medida para mejorar su postura de seguridad.

- **¿CÓMO SE HACE?**

1. Registramos a los usuarios en la plataforma Eslabón CDA (3BN).
2. Se envía un comunicado con las instrucciones de acceso a su equipo de trabajo manifestando la importancia y obligatoriedad de tomar el test. ***El tiempo límite es de 20 días***.
3. Eslabón CDA (3BN) calcula de forma automática las estadísticas y nos entrega un informe de gran valor.
4. El informe será presentado a la gerencia y personal de TI.

- **¿EN QUÉ CONSISTE?**

Utilizamos el test CDA que mide el coeficiente de detección de amenazas de los usuarios y además permite iniciar el proceso de concientización de una forma rápida, medible y

constructiva al 100%. Los usuarios enfrentan el reto de resolver un test con preguntas de sentido común y otras académicas que los motivará a buscar en internet aspectos relacionados con la ciberseguridad. Al finalizar el proceso se adquiere un alto nivel de conciencia ya que es la persona quién identifica su ignorancia frente al tema y la necesidad de capacitarse**.**

FASE 2 – CREACIÓN DE CONCIENCIA CON CHARLAS VIRTUALES DE SEGURIDAD DIGITAL

Las compañías necesitan un plan de acción inmediato que les permita entrenar a los usuarios para reconocer y saber qué hacer ante técnicas sofisticadas de ingeniería social, brute force, phishing, spear phishing, vishing, smishing, baiting y CEO Fraud; que han probado ser muy efectivas para obtener información sensible y perpetrar un ataque informático.

- **¿CÓMO HACERLO?**

1. Separe un espacio de 1 hora.
2. La charla se dicta de forma virtual.
3. Se entrega la grabación de la charla para repasar en casa una vez finalizada la sesión.

FASE 3 – ENTRENAMIENTO AVANZADO

1. Desarrollar un conocimiento sólido en seguridad digital.
2. Evidenciar las actividades - Cumplimiento.
3. Certificarse como usuario digital seguro.

¿EN QUÉ CONSISTE?

1. Cultura en ciberseguridad: 12 módulos de estudio que ayudan a corregir malas prácticas de seguridad.
2. Seguimiento al usuario: Visualice en el panel de administración el avance en las actividades realizadas por los usuarios y el administrador.
3. Repositorio de evidencias: Visualice que realmente se ejecuten las tareas.
4. Estadísticas: Identifique las áreas de la empresa que requieren atención, obtenga informes de valor para la gerencia.
5. Hoja de Ruta: Obtenga una guía base para desarrollar su programa de entrenamiento.
6. Herramientas: Obtenga campañas en ciberseguridad y úselas de fondo de pantalla o envíelas por correo.

7. Cumplimiento: Gestión centralizada de todas las actividades de entrenamiento a usuario final, ideal para cumplir con ISO 27001 / CONPES 3995.

FASE 4 – SEGURIDAD OFENSIVA

Son campañas enviadas por correo que utilizan los piratas informáticos como anzuelo para que el usuario entregue información o infecte su equipo. Las campañas son dirigidas a usuarios específicos que se les hace un seguimiento previo encontrando aspectos relacionados a gustos, forma de pensar, información que comparten, entre otras, desarrollando una campaña maliciosa "imposible" de evadir.

¿POR QUÉ HACERLO?

Una empresa que ha capacitado a sus usuarios para detectar correos maliciosos comenzará a descartar ataques de Phishing típicos. Los Hackers usarán entonces un ataque más especializado imposible de evadir ya que la información contenida en el email será familiar para el usuario. Es importante realizar este tipo de ataques y explicar en campañas como defenderse.

Una vez realizado el diagnóstico, las charlas, el entrenamiento con ESLABON CDA y la seguridad ofensiva con Spear Phishing Usted. habrá **avanzado satisfactoriamente 5 escalones** en la metodología de concientización en ciberseguridad (MECCI). Esta metodología contempla el proceso completo que debe atravesar un usuario hasta convertirse en un *"usuario digital seguro"*.

Digital User
Ciberseguridad para todos

PROPUESTA ECONÓMICA

FASE	DESCRIPCIÓN	INVERSION
Diagnóstico	Realizar un “Diagnóstico” utilizando el “instrumento de evaluación MSPI”. Fundamental para la fase de planificación. Incluye Análisis de vulnerabilidades en la red LAN y Seguridad Perimetral de la empresa.	**$ 27.700.500**
Planificación	Elaborar Plan de Seguridad y Privacidad de la Información con el objetivo de que la Entidad realice la planeación del tiempo, recursos y presupuesto de las actividades que va a desarrollar relacionadas con el MSPI.	**$ 34.000.000**
Operación	Implementar los controles, con el fin de dar cumplimiento con los requisitos del MSPI.	**$ 31.000.000**
Evaluación de Desempeño	Evaluar la efectividad de las acciones tomadas a través de los indicadores definidos en la fase de implementación que debe incluir la correcta interacción entre el MSPI	**$ 31.000.000**
Concientización Usuarios Finales	Aplicar estrategias y modelos de capacitación y concientización en ciberseguridad y seguridad digital según guía 14 del MSPI - Diagnóstico en ciberseguridad para 300 usuarios. - Paquete de 12 charlas de 1 hora en ciberseguridad. - Entrenamiento nube avanzado y certificado para 300 usuarios finales. Ataques Phishing para 300 usuarios.	**$ 26.715.500**
TOTAL PROPUESTA ECONOMICA - IVA INCLUIDO		**$ 150,416,000**

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

El proyecto se estima puede durar 10 - 12 meses.

Adicional: Se dispondrá de una persona medio tiempo (4 horas) de lunes a viernes para realizar apoyo en la elaboración de la documentación requerida para el presente proyecto.