MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

Este documento se realizó teniendo como base el -Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL- el cual contiene toda la información recopilada de la implementación de un modelo de seguridad basado en las necesidades y el tamaño de la estructura de la entidad.

“El Modelo de Seguridad y Privacidad de la Información – MSP, preserva la confidencialidad, integridad, disponibilidad y privacidad de la información, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos”.

El alcance de este documento es poder contar con un diagnóstico y adecuación del dicho modelo de seguridad dentro de la corporación de cultura y turismo. Revisar las falencias que pueda tener el modelo actual de seguridad y dar una serie de recomendaciones para pasar de la fase de diagnóstico a la fase de implementación.

OBJETIVO
Cumplir en un alto porcentaje con el modelo de seguridad y privacidad de la información en un mediano plazo.
Dar lineamientos para la implementación de la gestión de la seguridad y privacidad de la información.

DESARROLLO DE LAS ETAPAS PREVIAS A LA IMPLEMENTACIÓN

ESTADO ACTUAL DE LA ENTIDAD
El nivel de madurez en el que se encuentra en este momento la entidad es: Preparación. Esto obedece a determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad. Además de realizar levantamiento de información para las pruebas de efectividad que permitan a la Entidad medir los controles existentes.

ENCUESTA DE SEGURIDAD

5.1 Infraestructura física, acceso y medio ambiente.

a. Centro de Datos. Definir qué es un centro de datos y averiguar si en la entidad existen o no.

Un centro de datos es un lugar o espacio dedicado a la recolección de todos los datos de la empresa, tanto para su funcionamiento como para su almacenamiento. En la Corporación de Cultura y Turismo se cumple parcialmente con la solicitud de tener un centro de datos, ya que se tiene una copia de seguridad programada en un disco duro pero no es suficiente para dar cumplimiento a este requerimiento. Se debe contar con una copia automática en un servidor ubicado en un lugar óptimo con las características que exige dicho espacio.

b. Control de Acceso.

Se denomina control de acceso a lo que un sujeto puede hacer. La aprobación del acceso garantiza el acceso durante las operaciones, mediante la asociación de usuarios con los recursos que a los que están autorizados a acceder, basándose en la política de autorizaciones.

En la entidad se cuenta con un control de acceso muy deficiente, ya que está simplemente al inicio de cada equipo de cómputo, pero al acceder cualquier usuario tiene disponible toda la información.

c. Barreras.

En la entidad si existen barreras físicas que aíslan las áreas coyunturales de la entidad. Ya que existen puertas con seguridad en los equipos de mayor riesgo en la información, además de contar con candados en los racks de comunicaciones.

d. CCTV.

La entidad no cuenta actualmente con un circuito cerrado de televisión, casi su totalidad se encuentra desprotegido.

e. Cableado y Canaletas
   i. Datos. El cableado de datos se encuentra en su totalidad por canaletas, existen algunos unos puntos críticos los cuales están descubiertos, y se debe hacer una inversión para comprar e instalar las canaletas caídas o rotas.

ii. Eléctrico.

Existe cableado eléctrico en gran porcentaje de construcción, el edificio es antiguo, por tal motivo no cumple con muchas de las reglas actuales de la RETIE. Existen partes críticas que se encuentran en riesgo ya que se encuentran descubiertas.

f. Seguridad Perimetral. ¿Existe un Firewall en la entidad y se entiende para qué debe existir?

Actualmente como seguridad perimetral se cuenta con un antivirus de alta capacidad, el cual se hace su actualización de bases de datos mínimo una vez al mes. Los Firewall con los que se cuenta, es con los de cada equipo, no se cuenta con un firewall general y cabe mencionar que al tener más de la mitad de los equipos de la entidad obsoletos, se hace imposible garantizar la seguridad dentro de la red.

g. Switches y Hubs.

La red actual se compone de una entrada de red, la cual ingresa a un switch que distribuye la señal a cada uno de los equipos. También se cuenta con dos redes wifi las cuales parten desde ese Hub, una de ellas se encuentra con seguridad WPA y la otra red se encuentra sin seguridad.

h. Equipos en el Piso (fotos).
Actualmente se tienen 2 de los 15 equipos en el piso.

i. Aire Acondicionado.

No es necesario el uso de aire acondicionado, ya que el clima alcanza a ser solo templado y el edificio cuenta con muy buena ventilación, tiene techos altos y ventanas en todos sus costados. Adicional solo se cuenta con un rack donde están los switches y Hubs.

j. Reguladores y UPS.

Se cuenta con reguladores, con cortapicos y con UPS en la mayoría de los equipos. Existen actualmente tres equipos a los cuales se les dio de baja su respectiva UPS, por lo tanto se hace necesario reemplazarlas.

k. Planta de Emergencia. ¿Hay planta de generación de emergencia?

No se cuenta con planta de generación de emergencia, cada UPS proporciona alrededor de entre 10 y 20 minutos.

5.2. Lógico

l. Actualización de Servidores

Actualmente no se cuenta con servidores dentro de la entidad, toda la información necesaria de la página web se encuentra en servidores externos. Se tiene conocimiento de parchar y actualizar los servidores en caso tal de tenerlos con métodos como el YUM, WSUS o manual.

m. Pruebas de Intrusión.

Un Test de intrusión detecta el grado de seguridad real que tendría un atacante con intenciones maliciosas. El principal objetivo es saltarse todas las capas de seguridad en un sistema hasta conseguir acceso a la información más sensible de una empresa. Hasta el momento no se han hecho pruebas de intrusión al sistema de la corporación.

n. Hacking Ético

El Hacking ético consiste en vulnerar el sistema pero con fines de hacerlo más seguro, esto se hace externa o internamente, con el único fin de encontrar las partes vulnerables del sistema y poderlas corregir, actualmente no se ha hecho dentro de la corporación.

o. Ingeniería Social

La Ingeniería social es la práctica de obtener información confidencial a través de la

manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes informáticos, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos. El principio que sustenta la ingeniería social es el que en cualquier sistema "los usuarios son el eslabón débil". La ingeniería social dentro de la entidad se ha hecho a un nivel muy bajo, capacitando a los usuarios sobre los riesgos que enfrentan al recibir información no verificada.

5.3 Metodológico.

Averiguar cuáles de los siguientes puntos metodológicos existe y se utilizan en la entidad.

p. Políticas. ¿Hay un manual como tal? - No existe un manual en términos de seguridad.

q. Procedimientos. ¿Para qué labores? - No hay procedimientos definidos en el área de sistemas.

r. Normas. ¿Cuáles? - No existen normas actualmente.

s. Estándares. ¿Aplicados a qué? – No se cuentan con estándares.

t. Concientización. ¿Hacen regularmente procesos de concienciación en lo referente a seguridad de la información? ¿Se hace inducción a los empleados nuevos? – Se realizan procesos de inducción y re inducción sobre generalidades de la entidad, sin embargo en temas referentes a la Seguridad y Privacidad de la Información no se realizan actividades.

u. Acuerdos de Confidencialidad. ¿Los hay como tal o están embebidos en el contrato laboral? - Existen partes de los contratos laborales que se refieren al manejo de la información, se deben modificar o adicionar para hacer énfasis en la seguridad informática.

v. Renuncia de Propiedad de Información. ¿Se ha firmado aparte o existe dentro del contrato laboral? - Existen partes que hacen referencia a la información de la entidad y al manejo de la misma.

w. Código de Buena Conducta. ¿Existe? – Se cuenta con un código de Etica, sin embargo para procesos de seguridad y privacidad en la información no.

x. Metodología de Riesgos? – No

y. Metodología de Gestión de Activos? – Solamente para el manejo y custodia de archivos físicos de los procesos, en materia digital no se cuenta con procedimientos o acciones para garantizar su conservación.

z. Plan de Tratamiento de Riesgos? – No.

Mauricio Campillo Rojas
Ingeniero Electrónico