ASF Auditoría Superior de la Federación
CÁMARA DE DIPUTADOS

Dirección General de Auditoría de Tecnologías de la Información y Comunicaciones

Hallazgos y Recomendaciones en Materia de Seguridad de la Información

Lic. Genaro Héctor Serrano Martínez

Director de Auditoría de Tecnologías de Información y Comunicaciones

Declaraciones

“La información es un activo vital para las organizaciones, pero no siempre es reconocida como tal”

“La incapacidad de poder visualizar los efectos de la pérdida de información crítica puede dar lugar a importantes consecuencias”

“El grupo estratégico de seguridad de la información deberá asegurarse de que se integren los controles de seguridad en los equipos del ambiente operativo y de comunicaciones de la organización”

Cibercrimen en cifras

- En 2009, la mayor estafa de tarjetas de crédito en la historia comprometió más de 130 millones de cuentas
- La situación empeoró en 2011 cuando los datos de 117 millones de cuentas de usuario de Linkedin fueron robados
- En 2013, los datos de 500 millones de usuarios de Yahoo se filtraron en una de las brechas de datos más grandes de la historia
- En 2016, el ataque a Mossack Fonseca resultó en el compromiso de 11,5 millones de datos privados de los usuarios
- El costo de la ciberdelincuencia aumentará a US $ 2.1 billones en 2019, tres veces más que los ingresos de la delincuencia tradicional

Agenda

- **Estado de las Regulaciones en México**
- **Principales Responsabilidades de los Funcionarios**
- **Principales Hallazgos**
  - **Seguridad de la Información**
  - **Ciberseguridad**
  - **Continuidad de las Operaciones**
  - **Privacidad de Datos**
- **Recomendaciones**
- **Conclusiones**

Regulaciones

LEY DE SEGURIDAD NACIONAL

- **Desarrollar tecnología especializada para la investigación y difusión confiable de las comunicaciones del Gobierno Federal en materia de Seguridad Nacional, así como para la protección de esas comunicaciones y de la información que posea**

- **Definir las medidas de protección, destrucción, códigos de seguridad en las comunicaciones y demás aspectos necesarios para el resguardo de la información**

Regulaciones

MAAGTICSI

- **Proceso de Administración de Servicios (ADS)**
  - **Administrar la capacidad de la infraestructura de TIC**
  - **Administrar la continuidad de los servicios**

- **Proceso de la Seguridad de la Información (ASI)**
  - **Establecer el modelo de gobierno de la seguridad**
  - **Diseño del Sistema de Gestión de Seguridad de la Información (SGSI)**
  - **Elaborar el análisis de riesgos**

Regulaciones

LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA

- **Toda la información pública generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados es pública y será accesible a cualquier persona**

- **Como información reservada podrá clasificarse aquella cuya publicación comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable**

Regulaciones

LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

- **Con independencia del tipo de sistema en el que se encuentren los datos personales, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales**

- **El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad**

Responsabilidades

LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA

- **Establece los criterios para calificar las sanciones conforme a la gravedad de la falta, en su caso, las condiciones económicas del infractor y la reincidencia. Asimismo, contempla el tipo de sanciones, los procedimientos y plazos para su ejecución. Las sanciones de carácter económico no podrán ser cubiertas con recursos públicos**

LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

- **Se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos**

Responsabilidades

MAAGTICSI

- **Establecer y vigilar los mecanismos que permitan la administración de la seguridad de la información de la Institución, así como disminuir el impacto de eventos adversos**

- **El responsable del diseño de servicios de TIC, conjuntamente con el responsable de la planeación estratégica de la UTIC, deberán asegurarse que se cumpla con estándares para el Cifrado de Datos**

Responsabilidades

MAAGTICSI

- **En las contrataciones relacionadas con servicios de plataformas de procesamiento de datos, las Instituciones deberán prever que la administración e infraestructura esté clasificada en zonas de seguridad basadas en funciones, tipo de datos y requerimientos de acceso a los espacios de almacenamiento**

- **El grupo estratégico de seguridad de la información deberá asegurarse de que se integren al SGSI, controles de seguridad en los equipos del ambiente operativo y de comunicaciones de la Institución, para efectuar la revisión a las bitácoras internas de los mismos, con la finalidad de identificar intentos de ataques o de explotación de vulnerabilidades**

Hallazgos – Seguridad TI

Condición	Efecto
Falta de un responsable de seguridad para el cumplimiento de lo mecanismos de control, acciones de seguridad y administración de riesgos, entre otros	Ausencia de la función para vigilar la integridad, confidencialidad y disponibilidad de la información
Usuarios con acceso ilimitado a los aplicativos y bases de datos principales sin los controles pertinentes	Se pueden ejecutar transacciones no autorizadas sin dejar rastros

Hallazgos – Seguridad TI

Condición	Efecto
Carencia de políticas de seguridad institucionales, así como de normativas para su aplicación en todas las unidades y órganos de las entidades	Las estrategias de seguridad son heterogéneas y en algunos casos se contraponen
La administración de contraseñas tiene deficiencias como sesiones duplicadas, permite múltiples intentos fallidos, claves simples y repetitivas	El acceso a los aplicativos se encuentra en riesgo de accesos no autorizados

Hallazgos – Seguridad TI

Condición	Efecto
Carencia o deficiencias en la implementación del Sistema de Gestión de Seguridad de la Información (SGSI)	Pérdida de la confidencialidad de la información, falta de integridad de los datos, carencia de disponibilidad de las aplicaciones y falta de “no repudio” de las transacciones para deslindar responsabilidades
Se carece de recertificación periódica de usuarios y sus privilegios en los aplicativos sustantivos	Transacciones no autorizadas de acuerdo al rol del funcionario, así como ataques por parte de empleados dados de baja

Hallazgos – Seguridad TI

Condición	Efecto
Carencia del análisis de riesgos para evaluar su impacto sobre los servicios de la Institución, para obtener planes de remediación y definir los controles requeridos	Alto riesgo de materialización de las amenazas
Deficiencias en la gestión de incidentes que impide la identificación de los problemas con mayor frecuencia	Se obstaculiza la prevención de riesgos, así como los mecanismos de respuesta para mitigarlos.

Hallazgos – Seguridad TI

Condición	Efecto
Las pistas de auditoría y las bitácoras de los sistemas sustantivos no están activadas para su revisión periódica	No se detectan oportunamente los movimientos irregulares o cambios no autorizados
Los proveedores tienen acceso ilimitado a los aplicativos y bases de datos principales de la institución, sin la supervisión adecuada por parte de las entidades	Se pueden ejecutar transacciones no autorizadas sin dejar rastros que ponen en riesgo los activos y procesos de las instituciones
Carencia del análisis de Segregación de Funciones en las actividades de las áreas de TIC y en los procesos de negocio	No se detectan las actividades con posibilidad de fraude, irregularidades en los procesos o manipulación de los reportes financieros

Hallazgos – Ciberseguridad

Condición	Efecto
Deficiencias en el código de los servicios web que permiten accesos no autorizados para modificar la información restringida, así como la inyección de código malicioso	Expone el contenido del servidor así como a los usuarios que usan el servicio
Deficiencias en la configuración de los servidores que facilitan el acceso para provocar un mal funcionamiento	Se puede tener acceso a información sensible para la operación del sistema que podría afectar su funcionalidad

Hallazgos – Ciberseguridad

Condición	Efecto
La información se encuentra expuesta en el sitio web, por lo que se puede acceder a ella a través de buscadores convencionales	Existe el riesgo de suplantación de usuarios para acceder a contenido restringido.
Carencia de un análisis de vulnerabilidades de la infraestructura tecnológica y los aplicativos sustantivos	No se atienden o mitigan los riesgos asociados a un entorno en constante cambio que pueden afectar a los activos y operaciones de la entidad

Hallazgos – Continuidad

Condición	Efecto
Carencia de un centro de cómputo alterno con la capacidad suficiente para soportar de manera activa al centro de cómputo primario	Ante un desastre los mecanismos de recuperación presentarían fallas sustanciales y el tiempo objetivo de recuperación (RTO) sería mayor al estimado en los planes de contingencias
El centro de datos principal carece de la seguridad física suficiente para la operación de los servicios, con irregularidades en los sistemas de prevención de incendios, vigilancia, control de accesos, inundación, entre otros	La continuidad de la operación se encuentra en riesgo de ser interrumpida por un tiempo indeterminado

Hallazgos – Continuidad

Condición	Efecto
Deficiencias en la gestión de la disponibilidad de la infraestructura de cómputo para optimizar y monitorizar los servicios	No se asegura la operación de los procesos y sistemas con la finalidad de cumplir con los niveles de servicio establecidos
Carencia o falta de pruebas del Plan de Recuperación de Desastres (DRP) para identificar los servicios que podrían resultar afectados como consecuencia de interrupciones	El punto objetivo de recuperación (RPO) y el tiempo objetivo de recuperación (RTO) de la información, serían mayores a los soportados por la institución para la continuidad de las operaciones

Hallazgos – Continuidad

Condición	Efecto
Los respaldos no son probados periódicamente para detectar fallas en la grabación de los datos	El punto objetivo de recuperación (RPO) de información sería mayor al estimado en caso de una catástrofe en el centro de datos.
Se carece de un análisis de impacto al negocio (BIA) que considere todas las áreas sustantivas de la institución	Falta de identificación de las necesidades de recuperación para cumplir con los requerimientos de la organización, la jerarquía de prioridades y la propuesta de valor para soportar las inversiones y operaciones de la entidad
La gestión de la capacidad de la infraestructura tecnológica es deficiente para asegurar que los servicios cuentan con un procesamiento y almacenamiento suficiente	Los recursos no se aprovechan adecuadamente con la consecuente degradación de los niveles de servicio

Hallazgos – Privacidad

Condición	Efecto
Se carece de mecanismos de cifrado de datos en los dispositivos electrónicos móviles que contienen información reservada o sensible para la Institución	Alta vulnerabilidad para la privacidad de la información, tal es el caso del correo electrónico institucional
No se ejecuta el borrado seguro de la información para eliminar de manera permanente y de forma irrecuperable los datos contenidos en medios de almacenamiento y equipos de cómputo relacionados	Alto riesgo sobre la confidencialidad de los datos que puede derivar en el uso indebido de la información
No se clasifican los datos con la finalidad de determinar los niveles apropiados de control	La estrategia para asegurar la confidencialidad y privacidad de la información no es eficiente

Hallazgos – Privacidad

Condición	Efecto
Los usuarios acceden a información que no les corresponde de acuerdo con sus funciones y responsabilidades	No se protegen los activos de información de acuerdo a su prioridad y relevancia para la institución
Se carece de mecanismos de cifrado en las bases de datos sustantivas del Centro de Datos Principal	La integridad de los datos críticos o sensibles para la institución se encuentra en riesgo debido a que pueden ser alterados con facilidad, provocando pérdidas económicas y fraudes

Recomendaciones–Seguridad TI

- **Identificar y comprender las vulnerabilidades del entorno de la Seguridad, tanto humanas como técnicas**
- **Entender la causa y efecto de los riesgos para determinar el impacto que representan para la infraestructura tecnológica**
- **Aplicar los resultados del análisis de riesgos para determinar los activos que deben ser tratados primero y para cuales puede permitirse absorber el riesgo asociado a ellos**
- **Enfocar la gobernanza de TI, la seguridad y las inversiones en privacidad en las áreas que más contribuyen al cumplimiento de la misión de la entidad**
- **Conozca los datos de la organización, comprenda los datos que posee y qué está en riesgo.**

Recomendaciones–Seguridad TI

- **Restringir el acceso a la infraestructura tecnológica de acuerdo con el principio de “privilegio mínimo”, y garantizar que los administradores y los empleados sólo tengan los accesos y privilegios suficientes**

- **La alta dirección debe asegurarse de que el equipo de seguridad de la información obtenga un grado de visibilidad amplio respecto a todas las funciones de la entidad, mediante el reconocimiento de la importancia fundamental y prioritaria de la gestión de la seguridad para la organización**

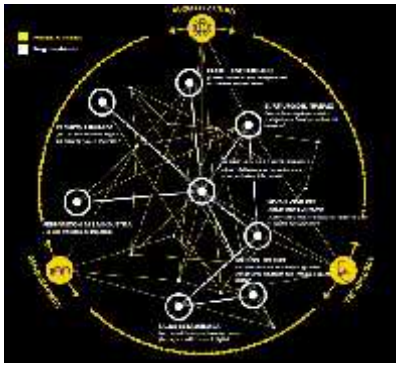
- **La prioridad del equipo de seguridad de la información es identificar las áreas de bajo y alto riesgo en la organización. Los marcos de riesgo deben alinearse estrechamente con la gestión organizacional y los proyectos en marcha**

Recomendaciones–Ciberseguridad

- **El equipo de evaluación debe utilizar un enfoque basado en el riesgo para concentrar la energía de auditoría en las áreas de mayor relevancia**
- **La gestión de cambios y parches debe enfocarse al conjunto de procesos ejecutados dentro de la organización para gestionar las mejoras**
- **La defensa en profundidad es una estrategia práctica para lograr la seguridad de la información en entornos altamente conectados como hoy en día**
- **La evaluación debe centrarse en el mayor riesgo e incluir medidas para reducir los falsos positivos.**
- **Debido a que los ataques pueden provenir de múltiples puntos, las evaluaciones deben incluir una revisión de las capas de seguridad de defensa en profundidad.**

Recomendaciones–Ciberseguridad

- Dado que las evaluaciones de seguridad informática deben probar un estado real contra un estado deseado, deben utilizar estándares
- Las víctimas no son sólo la organización, también la cadena de suministro, los clientes, sus familias y bancos
- El personal inexperto puede causar más daño que bien a la infraestructura tecnológica
- Aun cuando las evaluaciones de vulnerabilidad pueden consumir mucho tiempo, pueden salvar a la organización de una violación mayor causada por una vulnerabilidad
- Aplicar la denegación de servicio distribuida para la protección contra ataques



Recomendaciones–Continuidad

- La externalización de las operaciones de seguridad es una opción para organizaciones de tamaño medio, para reducir los problemas de mantenimiento en un escenario que siempre debe funcionar, sin perder de vista la gobernabilidad de los servicios y los acuerdos de no divulgación de la información

- Para las grandes organizaciones, siempre es mejor tener un equipo interno para las operaciones primarias de seguridad, debido a que el grado de confidencialidad de los datos involucrados es relativamente alto

- El programa de continuidad debe ser comunicado y coordinado con la institución para asegurar la alineación y eliminar la duplicación de esfuerzos.

- Los planes de continuidad deben ser actualizados para reflejar cualquier cambio significativo en los procesos de negocio, estructuras organizacionales e infraestructuras de TI

Recomendaciones–Continuidad

- **Las copias de seguridad deben ser probadas periódicamente para validar que los datos pueden restaurarse dentro de los RPO y RTO establecidos**
- **El programa de continuidad debe aprovechar las ubicaciones geográficas dispersas de la entidad para implementar la duplicación y sincronización de los datos en sistemas redundantes**
- **El entrenamiento y la concientización del programa de continuidad deben ser realizados periódicamente**
- **La entidad debe exigir a los proveedores de sistemas críticos que implementen y mantengan planes de continuidad que estén alineados con el plan de continuidad de la institución**

Recomendaciones–Privacidad

- Determinar cómo se recoge, utiliza, almacena y divulga la información personal
- La privacidad no puede existir sin la seguridad de la información, por lo tanto, debe considerarse en todos los programas de seguridad TI
- La privacidad debe ser parte del gobierno TI de la organización
- La capacitación es ampliamente aceptada por los expertos en privacidad como una de las facetas más importantes del programa

Recomendaciones–Privacidad

- Identificar los objetivos clave de privacidad de datos (principios y criterios), así como definir el alcance
- Evaluar a la gente, el proceso y la tecnología contra los objetivos de negocio definidos, e identificar áreas de mejora
- Documentar los resultados de la evaluación y las pruebas para que puedan utilizarse para apoyar las políticas de privacidad de la organización
- Proporcionar un equilibrio económico entre el impacto de la amenaza y el costo de la contramedida

Conclusiones

- **Es fundamental que las organizaciones se preocupen por posicionar estratégicamente a sus equipos de seguridad de la información, con las facultades y responsabilidades adecuadas para influir en los resultados de las entidades**

- **El Responsable de la Seguridad debe tomar el control de actuar como el integrador principal de la acciones en esta materia, para asegurar que los objetivos de la seguridad están bien alineados con las metas de la institución**

- **Reducir las ganancias del negocio del cibercrimen mediante la implementación de mejores soluciones de seguridad, equipar a los profesionales altamente calificados con las herramientas más eficaces y endurecer las leyes para tener sanciones efectivas**

Conclusiones

- **La privacidad es un factor inherente al ser humano que debe ser manejado en forma responsable y con las mejores tecnologías para garantizar que sólo las personas autorizadas puedan transmitirla**

- **Identificar las necesidades de continuidad y recuperación para cumplir con los requerimientos de la organización, la jerarquía de prioridades y la propuesta de valor para soportar las operaciones de la entidad**

Gracias

http://mx.linkedin.com/in/GenaroHectorSerranoMartinez

ghectorserrano@hotmail.com

@ghectorserrano