



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

INFORME DE ACTIVIDADES PROFESIONALES

PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

PRESENTA:

MARCOS JAIR FARFÁN PEÑALOZA

ASESOR: M. C. Alejandro Velázquez Mena

CIUDAD UNIVERSITARIA 2013

ÍNDICE

RESÚMEN	5
CAPÍTULO 1. INTRODUCCIÓN.....	7
1.1 Introducción.....	8
1.2 Trayectoria estudiantil.....	9
1.3 Selección de módulo de salida.....	9
1.4 Transición estudiantil al ámbito laboral	10
1.5 Objetivo del proyecto	10
CAPÍTULO 2. DESCRIPCIÓN DE PROYECTOS.	11
2.1 Supervisión de Seguridad Perimetral.....	12
2.2 Aplicación de políticas de control de acceso en un centro de cómputo.....	12
2.3 Instalación y configuración de Redes UMTS (Sistema Universal de Telecomunicaciones Móviles)	13
2.4 Logística y coordinación de proyectos UMTS.....	17
2.5 Atención de incidentes en la seguridad de la información.....	18
2.6 Análisis de riesgos.....	19
2.7 Coordinación de planes de mitigación de riesgos	20
CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	21
3.1 Descripción de la empresa	22
3.2 Dirección General en Seguridad	23
3.3 Equipo para la Gestión de Incidentes en la Seguridad de la Información.....	25
3.4 Toma de la función	27
3.5 Problemática y necesidades.....	32
3.6 Inventario de los procesos.....	34
3.7 Campo legal a cubrir.....	39
3.8 Implementación del programa GISI. (Gestión de Incidentes en la Seguridad de la Información)	41

3.9	Acuerdos y niveles de servicio	43
3.10	Análisis de riesgo.....	45
3.11	META del riesgo	52
3.12	Grado de difusión.....	53
3.13	Equipo de primera respuesta para Eventos en la Seguridad de la Información	55
3.14	Equipo para la Gestión de Incidentes en la Seguridad de la Información.....	57
3.15	Registro, seguimiento y cierre de los casos.....	60
CAPÍTULO 4. RESULTADOS.		63
4.1	Incremento en las notificaciones	64
4.2	Métricas.....	69
CONCLUSIONES		71
ÍNDICE DE FIGURAS.....		2
2.1	Topología de una red UMTS Ensenada Baja California	14
2.2	Topología de una red UMTS Nogales, Sonora	14
2.3	Propuesta de instalación de una antena UMST antes- después	15
2.4	Instalación de equipo Nodo B.....	16
2.5	Antenas UMTS instaladas	16
3.1	Organigrama Dirección General Seguridad	25
3.2	Categorías del Programa All	28
3.3	Etapas en el proceso de atención a eventos /incidentes.....	30
3.4	Diagrama de flujo del proceso de atención a eventos/incidentes	38
3.5	Matriz de nivel de riesgo.....	50
3.6	Software para el cálculo del nivel de riesgo.....	51
3.7	Minuta de asistencia a capacitaciones GISI	54
4.1	Porcentaje de atención por categoría	66
4.2	Datos no reales de no eventos atendidos durante un año	67
4.3	Datos no reales de eventos atendidos durante el primer año	67
4.4	Datos no reales de incidentes atendidos durante el primer año	68
4.5	Datos no reales relacionados a la distribución de casos atendidos por categoría durante el primer año.	69

ÍNDICE DE TABLAS.....	3
2.1 Tareas a realizar como parte de la coordinación de un proyecto UMTS	15
3.1 Tareas a desarrollar para la implementación del programa	42
3.2 Matriz de Impacto al prestigio.....	47
3.3 Matriz de probabilidad	48
3.4 Matriz de exposición	49
APÉNDICE	75
GLOSARIO.	77
REFERENCIAS.	83

Resumen

La presente descripción es un breve comentario con respecto al contenido del reporte ,dividido por cada uno de los cuatro capítulos que forman el presente documento:

Capítulo 1. Consta de una introducción al documento junto con el objetivo del proyecto, así como la panorámica del alumno durante y desde el egreso de la carrea

Capítulo 2. Consta de una descripción de las actividades realizadas durante toda la etapa profesional del estudiante, es decir, describe las funciones llevadas a cabo en cada uno de los empleos hasta el presente de la carrera laboral,

Capítulo 3. Consta de una descripción del organigrama la institución financiera dentro de la cual se implementa este proyecto, así como las actividades realizadas para la implementación del proyecto desde el inicio de este, con una descripción detallada de cada acción llevada a cabo junto con los principales problemas enfrentados con su respectiva solución.

Capítulo 4. Consta de la descripción de los resultados obtenidos durante el primer año de operación, así como una comparativa del trabajo hecho por la antigua administración con los logros obtenidos gracias a la correcta implementación del proyecto

CAPÍTULO 1.
INTRODUCCIÓN.

INTRODUCCIÓN.

1.1 Introducción.

A través de los años nuevas tecnologías de la información han sido creadas para facilitar las actividades cotidianas de los seres humanos, hecho que además de brindar comodidad a sus usuarios, ha beneficiado a la mayoría de las Instituciones alrededor del mundo en sus actividades laborales, sin embargo con éstos avances tecnológicos se han detectado vulnerabilidades y amenazas relacionadas a la seguridad de la información. Las tecnologías de información se han enfocado en el funcionamiento de los sistemas para su uso y explotación sin tomar en cuenta la operación de éstos dentro de un ambiente seguro, es por ello que no existe institución, sistema, proceso o ser humano en el mundo que no sea vulnerable a un intento de ataque lógico o físico dependiendo su naturaleza.

Con el gran avance tecnológico en el que vivimos, surge la necesidad de tomar en cuenta enfoques que anteriormente no tenían relevancia alguna para las instituciones que manejan información crítica en su operación como lo debe ser un funcionamiento de los sistemas, aplicaciones y procesos dentro de un ambiente seguro en donde se almacene información. Muchas organizaciones invierten grandes cantidades de dinero en tecnología para proteger su infraestructura y activos informáticos; sin embargo, estudios recientes han demostrado que han pasado por alto lo que representa hoy en día el mayor riesgo a la seguridad de la información, considerando ésta gran amenaza los propios seres humanos.

En México existe la gran necesidad de tomar en cuenta la protección a la información, tal como lo establece la ley reglamentaria en la materia vigente en el marco jurídico mexicano, que tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo y controlado, esto para garantizar la privacidad y el derecho a la autodeterminación informativa de las personas; esta ley enfatiza aún más, el tema de la seguridad de la información y obliga a todas las instituciones a cumplir con lo estipulado en esta ley, siendo la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (publicada el 5 de julio de 2010 dentro del Diario Oficial de la Nación)

La mayoría de las instituciones que han enfrentado ataques que han derivado en incidentes en la seguridad de su información, saben que cuando el incidente es detectado, la confidencialidad, verificación de integridad, disponibilidad y autenticidad de la información han sido afectadas y solo queda tratar de minimizar los daños que el incidente causó; por ello, contar con un equipo de especialistas encargado de cuidar los activos informáticos de una institución el cual tenga la capacidad de identificar amenazas y/o vulnerabilidades informáticas como por ejemplo los accesos

no autorizados, ataques de día cero, denegaciones de servicio, Ingeniería Social, fugas y/o pérdidas de información clasificada como confidencial así como otros posibles vectores de ataque, es sin lugar a duda un servicio fundamental que todas las empresas e instituciones dependiendo de la información que manejen deben tener en sus filas, esto con el objetivo de minimizar los posibles impactos negativos en cada una de las Empresas e Instituciones.

1.2 Trayectoria Estudiantil

Desde el primer día de mi estancia en la honorable Universidad Nacional Autónoma de México pasando por el bachillerato al proceso de ser seleccionado para estudiar mi licenciatura en Ciudad Universitaria y hasta mi último día de clases en Facultad de Ingeniería, tuve el compromiso de respetar esta gran Institución esforzarme al máximo en todas y cada una de las actividades que realicé como parte de mi formación académica dentro y fuera de sus instalaciones. La UNAM me brindó la oportunidad de tener una educación de muy alta calidad pidiéndome a cambio compromiso, esfuerzo y responsabilidad durante mi estancia en todos y cada uno de los años que fui su alumno, en donde aprendí a conocer en todas mi materias cursadas temas de gran trascendencia para la historia del mundo, las innovaciones tecnológicas que día a día le dan un giro a la sociedad, así como valorar el gran labor que se realiza dentro de nuestra máxima casa de estudios al formar grandes seres humanos con Ética y altamente competitivos.

Personalmente, terminar la licenciatura no fue sencillo ya que desde que el cuarto semestre en que me encontraba estudiando la carrera en Facultad de Ingeniería trabajé por mi propia cuenta arreglando equipos de cómputo para micro y medianas empresas, por lo que el desgaste derivado de la combinación entre mi trabajo y mis estudios representó un reto aunado a un mayor compromiso en todas las materias que curse, ya que en algunos semestres asistí a clases de lunes a sábado.

Mi estancia en Facultad de Ingeniería sembró en mí los fundamentos teóricos y prácticos relacionados a la carrera que cursé (Ingeniería en Computación), que gracias al entendimiento de estos temas nació en mi una nueva forma de pensar y actuar; con los cuales se formó mi carácter, personalidad y pensamiento crítico-analítico que hoy son la base de mi presente y que gracias a estos finalicé mis estudios en Junio del 2008.

1.3 Selección de Módulo de salida

Cuando cursé los últimos cuatro semestres de mi carrera en Facultad de Ingeniería, se aprobó un cambio de plan de estudios con opciones de especializaciones o módulos de salida entre los cuales fue de mi gran interés el módulo de “Redes y Seguridad”, este módulo captó mi total atención al ver las materias obligatorias y optativas que podía cursar ya que el tema relacionado a la Seguridad en ese momento era de mi total desconocimiento.

Sin embargo, derivado de las charlas que tuve con algunos de mis profesores en cuanto a la posible elección de ese módulo me motivaron a elegirlo por la estructura de su marco teórico descrito en el plan de estudios aunado al campo de trabajo que mis profesores visualizaron dentro del ambiente laboral para los próximos años. Una vez que tomé la decisión de inscribirme en este módulo de salida, al cursar las primeras materias supe que tomé la decisión correcta ya que las materias nombradas Seguridad Informática I y II sembraron en mí el interés de conocer más los temas vistos y ver la proyección a nivel laboral de estos.

1.4 Transición Estudiantil al ámbito laboral

Esta etapa de mi vida representó en mí un cambio en toda la extensión de la palabra, ya que cumplir con las responsabilidades escolares es un tema muy distinto a la interacción al ámbito laboral, para mi fortuna la primera Institución que me brindó la oportunidad de unirme a su equipo de trabajo me mostró que los conocimientos adquiridos en la formación académica son la base de un buen desempeño en cualquier Institución dentro del ámbito laboral, aunado al saber trabajar en equipo. Mi jefe directo de igual forma egresado de la UNAM me orientó en cuanto a trabajar con un nivel de calidad en todas aquellas tareas que me asignó como lo fue principalmente la supervisión de políticas de seguridad

En Julio del 2008 entre a laborar en una empresa dedicada a instalar tecnologías para infraestructura de telecomunicaciones como Ingeniero de redes inalámbricas en donde fui responsable a mi muy corta instancia de supervisar y configurar la tecnología de la empresa para la implementación de una UMTS, en donde los conocimientos que adquirí en mis clases de Redes Inalámbricas Avanzadas me apoyaron en cuanto al buen desempeño que tuve durante dos años.

En Julio del 2010 formé parte de una Institución Financiera como Ingeniero de Seguridad Informática en donde realicé la implementación de un equipo para la Gestión de Incidentes en la Seguridad de la Información, actividad que realicé hasta la fecha Enero del 2013

1.5 Objetivo del proyecto

El objetivo de este trabajo es implementar una guía para el manejo de incidentes en la seguridad de la información dentro de una institución financiera, de esta forma lograr que la institución se encuentre preparada para atender un incidente en la seguridad de la información cuando este se presente, así mismo contar con los aspectos necesarios para poder tener una gestión de un incidente teniendo como prioridad minimizar el impacto financiero y el impacto negativo a la marca generados por el incidente; de igual forma, lograr que progresivamente los empleados de la institución tengan claro qué y dónde reportar un incidente en la seguridad de la información.

CAPÍTULO 2

DESCRIPCIÓN DE PROYECTOS.

DESCRIPCIÓN DE PROYECTOS

2.1 Supervisión de Seguridad Perimetral.

Actividad realizada como parte de un proyecto nombrado “Seguridad en el Centro de Cómputo” Como primera experiencia laboral en una institución financiera durante el periodo de Agosto 2007 – Febrero 2008 como asistente en el centro de cómputo, consiste principalmente en la realización de análisis de riesgos con una metodología cualitativa institucional dentro de un centro de cómputo bajo las Políticas de Gobierno en Seguridad de la Información ya establecidas en la institución financiera con el objetivo de evaluar y supervisar la correcta segmentación de los perímetros físicos existentes, de la misma forma se realizan inventarios de los equipos de cómputo e inmobiliaria existentes para evaluar su permanencia dentro del centro de cómputo así como la supervisión de la instalación de cámaras de seguridad en puntos definidos mediante una evaluación a la ubicación de servidores en producción, con lo cual se definen los mecanismos de control de acceso para la autenticación a los perímetros físicos existentes dentro del centro de cómputo, perímetros en donde se encuentra equipo inmobiliario (escritorios, cajas de cartón, información no clasificada impresa) en los pasillos, los cuales son acomodados o retirados dejando libres los espacios del centro de cómputo.

De acuerdo a la existencia de tres perímetros físicos, esta actividad de supervisión perimetral clasifica los servidores críticos y se ubican mediante ventanas de mantenimiento en el perímetro interno del centro de cómputo, una vez realizada esta tarea se colabora en la supervisión de la instalación de las cámaras de seguridad monitoreadas por el personal de seguridad física realizando pruebas para encontrar puntos ciegos de las cámaras de vigilancia, acto inmediato posterior consta en realizar una serie de pruebas en un periodo de preproducción al mecanismo de control de acceso seleccionado a instalar (biometría mediante la identificación de huella digital) para controlar el acceso en todos los perímetros del centro de cómputo.

2.2 Aplicación de Políticas de Control de Acceso en un Centro de Cómputo.

Actividad realizada como parte de un proyecto nombrado “Seguridad en el Centro de Cómputo” en una institución financiera durante el periodo de Febrero 2008 – Julio 2008 como asistente en el centro de cómputo, esta modalidad de actividad consiste en la aplicación de las políticas de seguridad física existentes dentro del centro de cómputo con el objetivo de capacitar al personal de

seguridad física para el cumplimiento de las políticas de control de acceso al centro de cómputo, de igual forma restringir el acceso a personal no autorizado bajo los procedimientos internos de la institución financiera al centro de cómputo a manera de restringir el acceso de quipos telefónicos, memorias USB, cámaras fotográficas y grabadoras, lo anterior conforme a las políticas de control de acceso existentes en la Institución Financiera, esto con la colaboración y participación activa de oficiales de seguridad física máxime el descontento de los usuarios.

Al no contar con bitácoras de acceso al centro de cómputo, esta actividad se complementa creando un archivo en el que todos los empleados que entran al mismo deben de firmar una hoja impresa, escribiendo su nombre y autenticándose mediante la credencial del banco y su credencial de elector. Cabe mencionar que esta actividad se complementa con diversas bitácoras de áreas ajenas a efecto de cotejar y analizar una vez concluido el día laboral el acceso y salida del centro de cómputo, sirviendo a su vez éste cotejo para restringir accesos a becarios y personal no dado de alta en una lista blanca a realizar.

2.3 Instalación y configuración de Redes UMTS. Sistema Universal de Telecomunicaciones

Móviles

Actividad realizada como parte de cuatro proyectos nombrados “Red UMTS” en una importante empresa que fabrica equipo de redes y telecomunicaciones especializada en el desarrollo de implementación de nuevas tecnologías durante el periodo Julio 2008 – Octubre 2009 como Ingeniero de redes inalámbricas, esta actividad es llevada a cabo por parte del departamento de redes inalámbricas de la empresa con el objetivo de implementar la instalación, configuración, pruebas de servicio y entrega de una red UMTS (Universal Mobile Telecommunications System - Sistema Universal de Telecomunicaciones Móviles) tal y como se observa la Topología a la que se hace referencia en la (figura 2.1 y 2.2) a una importante empresa española que brinda servicios de telefonía móvil en las ciudades de Guadalajara, Ensenada, Culiacán y Hermosillo.

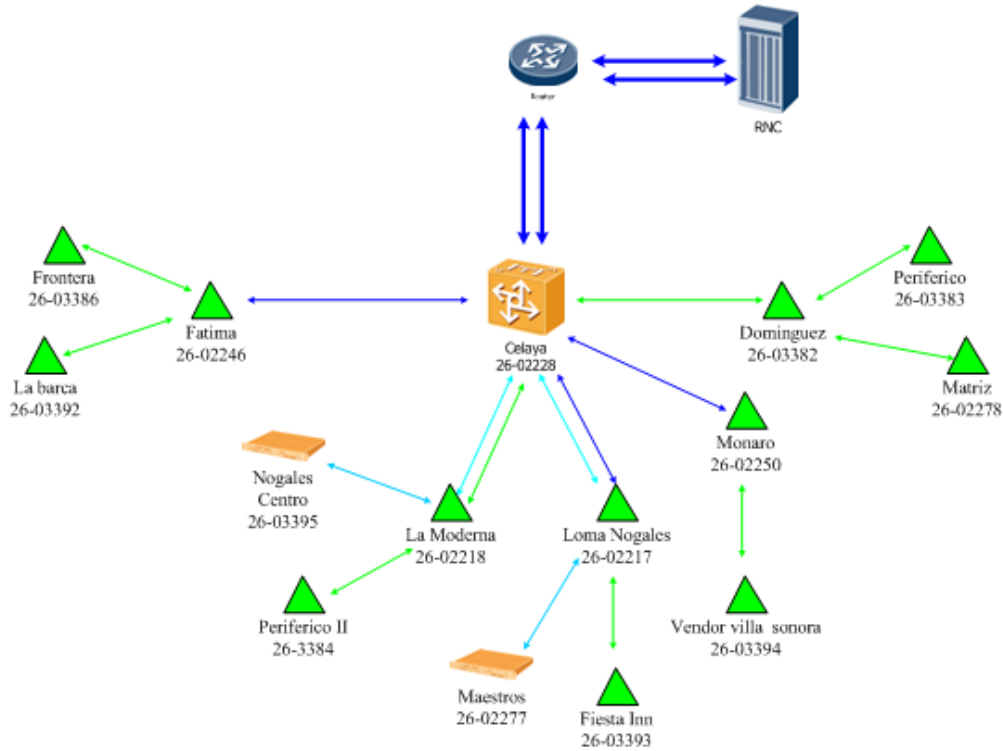


Figura 2.1 Topología de una red UMTS Nogales, Sonora

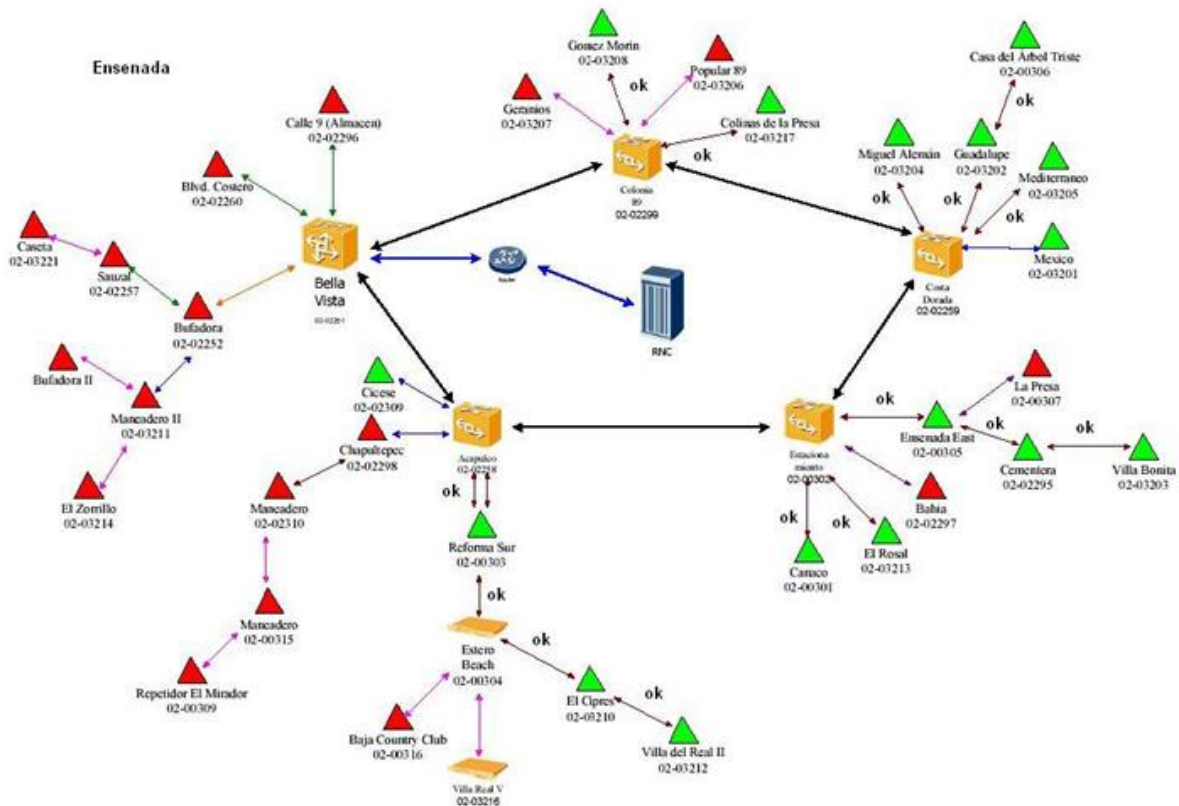


Figura 2.2 Topología de una red UMTS Ensenada Baja California

De igual forma se asigna a cada Ingeniero del departamento referido en el párrafo inmediato anterior, un equipo de proveedores los cuales realizan la instalación del equipo NODO B RED UMTS de acuerdo al tipo de Ingeniería de instalación previamente realizada entre el cliente y otra área de la empresa en donde se especifica la ubicación del equipo, altura de las antenas y espectro de cobertura de las mismas, trayectoria del cableado, así como las posiciones en los Racks existentes.

A su vez, se lleva a cabo la supervisión del material para la instalación de los equipos “Nodos B”, ya que en caso de alguna inconsistencia en la Ingeniería de Instalación, el ingeniero encargado del sitio debe de tomar la mejor decisión con base a un análisis con respecto a la trayectoria y posición de equipo a instalar conforme las normas del cliente tal como se ve en la (Figura 2.3), cabe mencionar que el hecho de tomar una mala decisión al respecto, da como resultado retrasos y penalizaciones económicas en la entrega de la red.

Una vez realizada la instalación y la verificación de la misma por parte del Ingeniero encargado del sitio el cual pertenece al departamento al que se está refiriendo, se enciende el equipo para configurar éste con el script mediante una aplicación propia de la empresa.

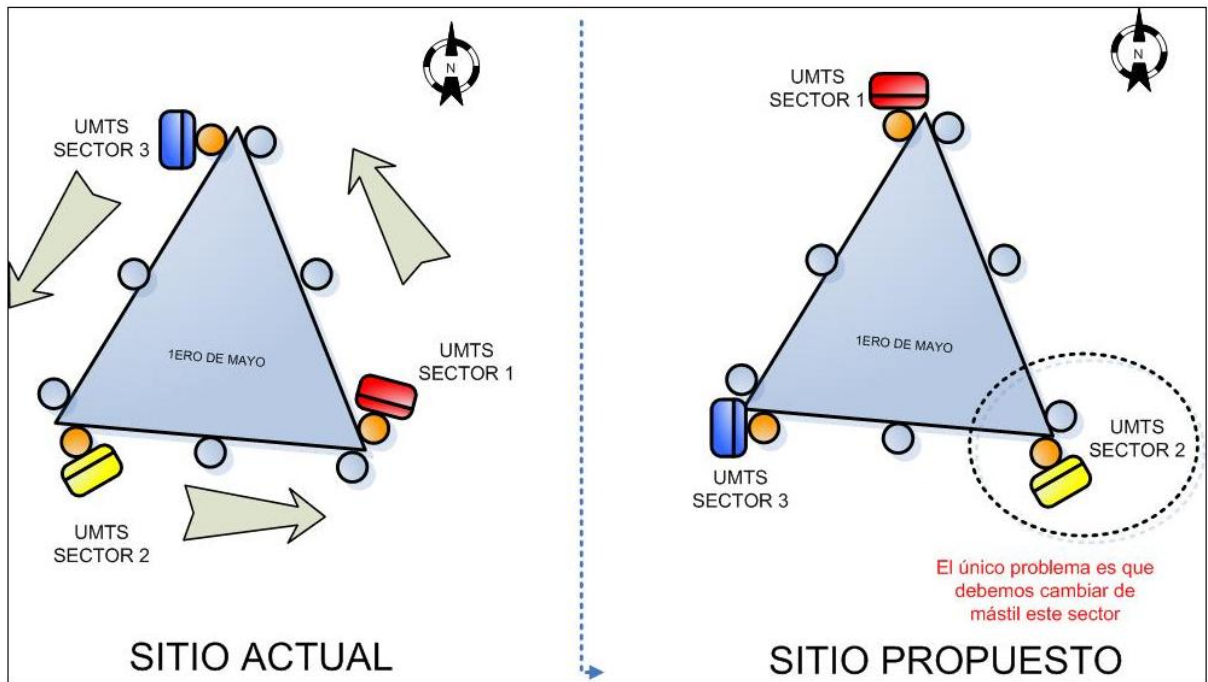


Figura 2.3 Propuesta de Instalación de una Antena UMTS Antes- Después

Aunado a lo anterior se realizan pruebas a los servicios de llamada, video llamada y datos de los tres sectores del Nodo B, ya que en caso de existir una falla del equipo, el Ingeniero a cargo debe realizar una inspección a fondo de toda la instalación, conexiones y configuración para determinar la causa de la falla, y en caso de resultar un material dañado, este se pide a una bodega de la empresa para volver a instalar el material indicado por el personal dependiente del Ingeniero a cargo.

Una vez terminado los puntos anteriores para todos los nodos a instalar en la ciudad y haber concluido la limpieza de los sitios en cada uno de ellos, se procede a realizar las entregas de los nodos al cliente, la cual consiste en revisar la posición del Nodo B (en caso de haber cambios por una inconsistencia en la Ingeniería justificarlos al cliente), revisar el cableado, la calidad de la instalación, verificar físicamente con el cliente la posición de las antenas tal y como se observa en la (figura 2.4 y 2.5), servicio de datos, servicio de llamadas y video llamadas; para que posteriormente se firmen las actas de aceptación de los sitios, actas que avalan el trabajo realizado por el equipo de trabajo perteneciente al grupo de Ingenieros integrantes del Departamento de Redes Inalámbricas.

Foto: NODO B Instalado

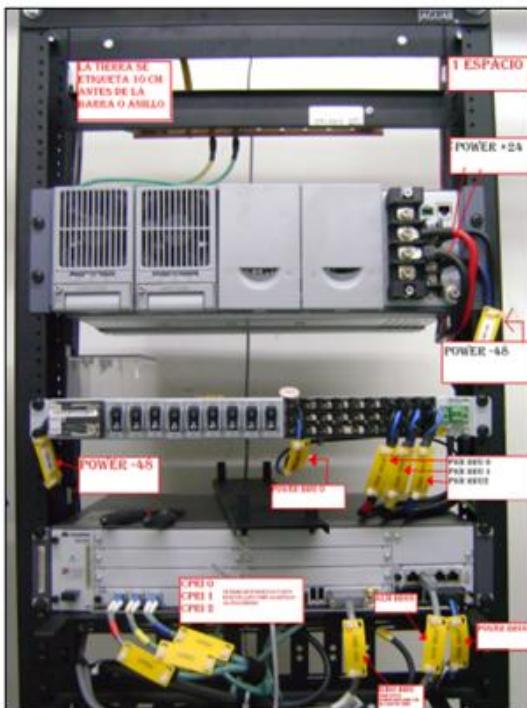


Figura 2.4 Instalación de Equipo Nodo B.

Foto: Soporte de Antenas Existente



Figura 2.5 Antenas UMTS Instaladas.

2.4 Logística y Coordinación de Proyectos UMTS.

Actividad realizada como parte de seis proyectos nombrados “Red UMTS Norte” en una importante empresa que fabrica equipo de redes y telecomunicaciones especializada en el desarrollo de implementación de nuevas tecnologías durante el periodo Octubre 2009 – Junio 2010 como Líder de proyecto, esta tarea consiste en llevar a cabo la logística, coordinación, supervisión del proyecto, UMTS (Universal Mobile Telecommunications System - Sistema Universal de Telecomunicaciones Móviles) a una importante empresa española que brinda servicios de telefonía móvil para las ciudades de Ensenada, La Paz, Guaymas, Nogales, Ciudad Obregón y los Mochis, con el objetivo implementar una red UMTS en cada una de las ciudades descritas, al tener como primer función realizar la correcta selección, distribución y evaluación de material para cada sitio en donde se instalan los “Nodos B” donde dependiendo del resultado de la Ingeniería hecha anteriormente por un departamento ajeno a este escrito, se organiza y se realiza una capacitación a todos los proveedores contratados por la empresa, esto con el objetivo de darles a conocer los equipos con lo que cuenta la empresa, la forma de trabajo conforme a la experiencia adquirida en otros proyectos con el mismo cliente ,bajo los estándares de instalación y normas de trabajo del cliente con el fin de optimizar el tiempo de instalación y entrega de la red.

A su vez se evalúan los sitios seleccionados por el cliente en donde se instalan los “Nodos B” para prever complicaciones durante la instalación, y en caso de ser necesario proceder a visitar al cliente con motivo de realizar una propuesta con el fin de modificar la Ingeniería y llevar a cabo el proceso de completo, hasta la entrega del sitio sin contratiempo alguno, supervisando toda esta actividad y reportándola a los altos mandos de la empresa tal y como se observa en Tabla de avance del proyecto (Tabla 2.1) . Este hecho optimiza el tiempo de vida del proyecto y reduce costos.

CAPÍTULO 2. DESCRIPCIÓN DE PROYECTOS.

Tabla 2.1 Tareas a Realizar como parte de la coordinación de un proyecto UMTS.

Task ID	Task Name	Resource Name	Work	Start	Finish	% Work Complete
3	PO Issue or Loan Contract (Site Adaption & Equipment 28 Node B, 1 RNC,84 Antennas)	Sales AM	8 hours	Mon 3/30/09	Mon 3/30/09	0%
4	Contract Application	Sales PLM	120 hours	Tue 3/31/09	Mon 4/20/09	0%
7	Network Planning Approval	Huawei RF	8 hours	Wed 1/14/09	Wed 1/14/09	100%
8	Confirm Spectrum Clearance	TEMM	0 hours	Fri 2/27/09	Fri 2/27/09	100%
13	Site List Approved	TEMM	8 hours	Fri 2/27/09	Fri 2/27/09	100%
14	Site Survey Report Template Review	Huawei SS	8 hours	Fri 2/27/09	Fri 2/27/09	100%
14	Site Survey Report Template Review	TEMM	8 hours	Fri 2/27/09	Fri 2/27/09	100%
15	Installation Standar Review	Huawei RAN	8 hours	Fri 2/27/09	Fri 2/27/09	100%
15	Installation Standar Review	TEMM	8 hours	Fri 2/27/09	Fri 2/27/09	100%
24	RNC Engineering	Huawei RAN	136 hours	Thu 4/23/09	Fri 5/15/09	100%
24	RNC Engineering	TEMM	136 hours	Thu 4/23/09	Fri 5/15/09	100%
25	Node B Engineering	Huawei RAN	136 hours	Thu 4/23/09	Fri 5/15/09	100%
25	Node B Engineering	TEMM	136 hours	Thu 4/23/09	Fri 5/15/09	100%
26	RNC & Node B Engineering Approved	TEMM	0 hours	Fri 5/15/09	Fri 5/15/09	100%
30	Node B Material Preparations (Supports)	Huawei PQD	80 hours	Mon 4/20/09	Fri 5/1/09	100%
31	Node B Site Adaptions CDMA Uninstallation	Huawei SS	40 hours	Mon 4/20/09	Fri 4/24/09	100%
32	Node B Site Adaptions Antenna Support Installation and Relocation	Huawei SS	56 hours	Mon 5/11/09	Tue 5/19/09	0%

2.5 Implementación de un Equipo de Gestión de Incidentes en la Seguridad de la Información.

Actividad realizada como parte del proyecto “Gestión de Incidentes en la Seguridad de la Información” en una institución financiera durante el periodo Junio 2008 – Octubre 2012 como Ingeniero en Seguridad Informática, esta tarea se lleva a cabo por parte de un equipo conformado por 2 personas y yo, asignadas dentro de la institución financiera con el objetivo de implementar un equipo para gestionar los incidentes que se presenten en la seguridad de la información. Este proyecto se realiza bajo un análisis de riesgos hecho con la metodología cualitativa institucional para conocer el estado actual del programa que tiene la Institución a efecto de gestionar los incidentes en la seguridad de la información, persiguiendo como prioridad evaluar el inventario de los procesos, el correcto apego ó desapego a las normas y estándares de la Institución, validar una matriz de contactos actualizada ó no, así como activos informáticos clasificados dentro de la Institución.

También es objeto por parte del Equipo de Gestión de Incidentes en la Seguridad de la Información analizar el marco legal aplicable y vigente al respecto a efecto de aplicar y cumplir con lo estrictamente establecido por las leyes regulatorias en la materia a efecto de dar cabal cumplimiento junto con todas las áreas involucradas de igual forma organizando reuniones con áreas de Tecnologías de Información, con el fin de realizar acuerdos de trabajo y niveles de

servicio fundamentales para el proceso de gestión de los incidentes como lo son los equipos de antivirus, los servidores de correo, las telecomunicaciones, la infraestructura, el monitoreo y Oficiales de seguridad de la información.

Como actividad adicional por parte del Equipo, se realizan análisis a los diagramas de flujo existentes de acuerdo los procesos vigentes a efecto de encontrar posibles faltas de información en los mismos, procediendo a actualizar todos los manuales de operación, diagramas de flujo, matrices de contactos, acuerdos de trabajo y niveles de servicio (OLA's & SLA's) en lenguaje Español e Inglés; de igual forma buscar trabajar con todas las áreas involucradas en un escenario o circunstancia en la que se requiera la recuperación y continuidad del Negocio, así como probar todos los acuerdos anteriormente citados.

2.6 Análisis de Riesgos.

Actividad realizada como parte del proyecto “Gestión de Incidentes en la Seguridad de la Información” en una institución financiera durante el periodo Octubre 2012 – Febrero 2013 como Analista en Seguridad Informática, esta tarea tiene como objetivo realizar análisis de riesgos a los activos informáticos usando la metodología cualitativa institucional basados en la protección de la Integridad, Confidencialidad y Autenticidad de la Información con el fin proteger los servicios de la información en una la institución financiera.

Cabe mencionar que cada que se presenta una situación en la que alguno estos tres servicios de la información referidos se encuentra en riesgo, se hace un análisis para enunciar el alcance del caso, de esta forma se da paso a realizar una investigación enfocándose en encontrar respuestas a las siguientes preguntas:

- ¿Qué ocurrió?
 - o Descripción de la afectación del reporte
- ¿Cómo ocurrió?
 - o Enfocado a conocer el detalle de los hechos reportados.
- ¿Cuándo ocurrió?
 - o Enfocado a conocer la fecha o fechas involucradas del reporte.
- ¿Dónde ocurrió?
 - o Enfocado a conocer la ubicación física, segmento de red, equipo tecnológico involucrado relacionados al reporte.
- ¿Por qué ocurrió?
 - o Enfocado a conocer la vulnerabilidad y amenaza involucrada.

- ¿Quién está involucrado?
 - o Enfocado a conocer a los posibles empleados, proveedores, infraestructura involucrada dentro del reporte.

Descrito lo anterior, una vez que se tienen identificadas las amenazas y/o vulnerabilidades detectadas, se les da una prioridad basada en la sensibilidad o criticidad de la información comprometida para estimar el impacto de amenaza y/o vulnerabilidad de cada caso en concreto. Una vez que se cuenta con dicha información, se deben identificar los controles necesarios para ejecutar acciones de mitigación, ya que el objetivo es llegar a la META del riesgo (Mitigar Evitar, Trasferir ó Asumir). Es oportuno mencionar que para los casos en los que no se cuenta con los controles necesarios para mitigar el riesgo existente referido, el equipo debe realizar un análisis costo-beneficio dando una prioridad a los resultados del análisis en base a la clasificación de la información, concluyendo con la elaboración de reportes ejecutivos del caso concreto reportado.

2.7 Coordinación de Planes de Mitigación de Riesgos.

Actividad realizada como parte del proyecto “Gestión de Incidentes en la Seguridad de la Información” en una institución financiera durante el periodo Octubre 2012 – Febrero 2013 como Analista en Seguridad Informática, esta actividad tiene como objetivo coordinar planes de mitigación de riesgos identificados previamente de manera conjunta y paralela con el negocio, debido a los posibles escenarios en donde se analizan casos en donde pudiese existir un fuerte riesgo para la Institución. Buscar mitigar el mismo puede implicar afectaciones a la operación del negocio, recordando y subrayando que la seguridad de la información no se encuentra por encima de éste; por ende, se procede a coordinar con las áreas afectadas buscando la mejor solución para mitigar el riesgo sin ocasionar un impacto a la operación de la institución financiera, por ello, una vez identificado el riesgo se coordina junto con todas las áreas involucradas en la detección de las amenazas y/o vulnerabilidades bajo un análisis aplicable a todo el ciclo de vida de todos los personal, sistemas, procesos y aplicaciones que estén involucrados, con el fin de llegar a una acuerdo en cuanto a las acciones para mitigar el riesgo, transferirlo o aceptarlo.

CAPÍTULO 3

IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

3.1 Descripción de la Empresa.

La Institución Financiera como empresa posee un gran prestigio debido a su sólida presencia en México, brinda servicios financieros a clientes corporativos e institucionales que se desempeñan en los mercados globales, servicios de banca corporativa e institucional, transacciones bancarias, depósitos y préstamos monetarios a pequeñas y medianas escalas. La Institución Financiera está catalogada como una de las Instituciones bancarias más importantes en nuestro país, teniendo una sólida presencia desde años atrás, cuenta con más de veinte mil empleados distribuidos en toda la república mexicana en todas sus sucursales de atención a clientes, cabe mencionar que posee una gran infraestructura tecnológica misma que es reflejada en su avanzada red de cajeros automáticos, contando con un poco más de seis mil en funcionamiento, la Institución Financiera cuenta con aproximadamente ocho y medio millones de clientes activos.

Así mismo dentro de la Institución Financiera se llevan a cabo acciones enfocadas al respeto del medio ambiente, el desarrollo social y la rentabilidad del negocio; por lo que se fomenta una filosofía corporativa basada en la ética, responsabilidad y sustentabilidad que benefician a los clientes, inversionistas y empleados, ya que permite establecer un modelo de generación de valor compartido favorable para los accionistas como lo son la economía, el medio ambiente y la sociedad ya que a través de éstos programas, se busca siempre lograr un mayor impacto social o ambiental posible, además de involucrar en ellos por medio de la participación de nuestros voluntarios.

En México todas las Instituciones Financieras se rigen por la Comisión Nacional Bancaria de Valores (CNBV), órgano dependiente de la Secretaría de Hacienda y Crédito Público (SHCP), el cual cuenta con autonomía técnica y facultades ejecutivas en los términos de la Ley de la Comisión Nacional Bancaria y de Valores, ley que tiene por objeto supervisar y regular en el ámbito de su competencia a las entidades financieras en México, a fin de procurar su estabilidad y correcto funcionamiento, así como mantener y fomentar el sano equilibrio del sistema financiero nacional con el principal fin de proteger los intereses del público al que ofrece sus servicios.

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

La Institución Financiera cuenta con una gran infraestructura, en nuestro país se divide en Direcciones Generales, las cuales a su vez están subdivididas en subdirecciones tal y como lo establece el estándar de la Institución para todas y cada una de las cedes en los países en donde tiene presencia. Por motivos de políticas de seguridad, es importante advertir que la información de Direcciones Generales está clasificada como información interna para uso exclusivo del personal autorizado por la Institución Financiera, por lo que para efectos del presente proyecto se dará a conocer únicamente la Dirección General a la que corresponde el presente trabajo, lo anterior, en virtud de existir impedimento de hecho y de derecho expreso al respecto.

Cada Dirección General tiene objetivos y distintas funciones, sin embargo, todas unen sus esfuerzos con el objetivo de mejorar su rendimiento y productividad enfocándose en brindar un servicio de calidad ya sea para los clientes o para los empleados. Cabe mencionar también que la Institución Financiera cuenta con una Dirección General en Seguridad Informática, en la cual se desempeñan labores de protección a la información de los clientes, se protegen los activos informáticos de la institución y se coordina una evaluación a los activos del negocio a efecto de establecer un parámetro para el manejo de los mismos. De igual manera la Institución Financiera maneja a diario de forma impresa, verbal y electrónica información que está considerada como uno de los activos de mayor valor para la Institución, la cual debe ser protegida en todas las etapas de su ciclo de vida, desde la creación, su procesamiento, almacenamiento y la destrucción de la misma.

3.2 Dirección General en Seguridad Informática.

La “Dirección General en Seguridad Informática” tiene por objetivo mejorar y mantener un perfil bajo en los riesgos de la información y de mercado bajo los lineamientos, políticas y estándares del Grupo Financiero en México y sus subsidiarias en los distintos países en donde tiene presencia, administrando sus pérdidas de crédito y riesgo contingente de mercado dentro de los parámetros o límites autorizados por el propio Grupo Financiero.

Esta Dirección General en Seguridad se integra de cuatro Subdirecciones, siendo éstas: La Subdirección de Seguridad Física, La Subdirección defraudes Informáticos, La Subdirección de Oficiales en Seguridad de la Información y La Subdirección en Seguridad de la Información, éstas cuatro Subdirecciones se encuentran divididas en Administraciones..

La Subdirección de Seguridad Física se encarga de controlar y/o restringir el acceso a todos los empleados que no estén autorizados para entrar a un perímetro físico, así como vigilar la entrada de equipos tecnológicos y activos ajenos a la Institución, también se encarga de autenticar a los empleados para el ingreso a los edificios y sus perímetros, tiene por función el monitoreo del sistema de circuito cerrado las veinticuatro horas del día, los siete días de la semana en todos los inmuebles.

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

La Subdirección de Fraudes Informáticos se encarga del monitoreo del sistema de red de los cajeros automáticos, este monitoreo contempla la detección de anomalías en los Cajeros Automáticos y el análisis del comportamiento de las tarjetas que son introducidas en los mismos bajo el sistema de la red bancaria, de igual forma se encarga de atender las reclamaciones de los clientes por montos no reconocidos en sus estados de cuenta o fraudes en general, realizando una investigación con el cliente para su protección y descartar posibles fraudes ficticios por parte de los tarjetahabientes; de igual manera se realizan investigaciones de campo por robos físicos en donde existió un compromiso de información, así como la realización de entrevistas a empleados maliciosos.

La Subdirección Oficiales en Seguridad de la Información está encargada de identificar las amenazas y vulnerabilidades en los procesos dentro las diferentes Direcciones de la Institución Financiera, éstos oficiales dentro de cada Dirección tienen como objetivo encargarse de las responsabilidades relativas a la seguridad y riesgo de la Información, realizando evaluaciones a la información que se maneja en sus áreas para administrar los riesgos de información a los que está expuesta su Dirección.

La Subdirección Seguridad de la Información se encarga del resguardo de la infraestructura tecnológica desde el punto de vista de la seguridad de la información, ésta subdirección tiene como funciones principales controlar el acceso a las aplicaciones de la Institución, altas y bajas de usuarios, restricciones a nivel aplicativo y realizar evaluaciones con respecto a la Seguridad de la Información a los proveedores o socios para tener acuerdos de confidencialidad de la información. Así mismo, de forma proactiva se encarga de la detección de amenazas y vulnerabilidades en contra de la infraestructura tecnológica de la institución para su pronta y oportuna gestión.

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

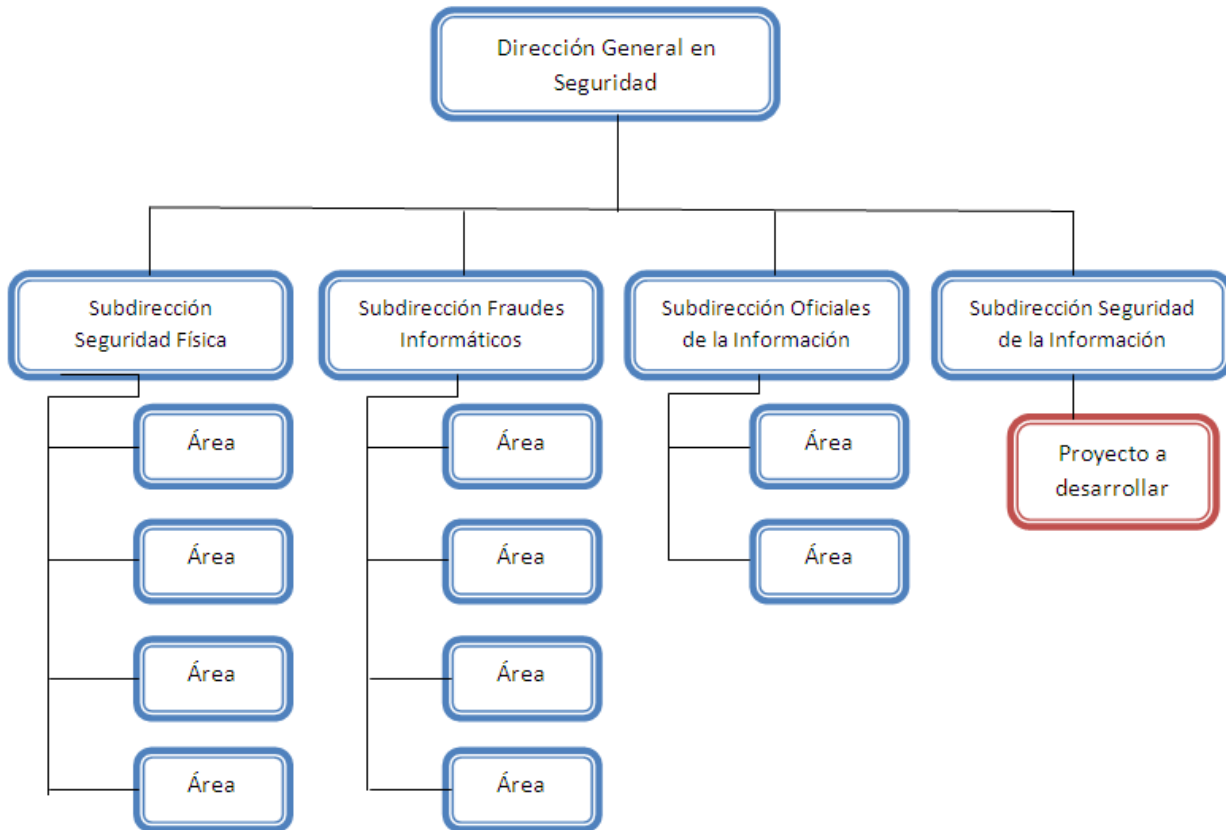


Figura 3.1 Organigrama Dirección General Seguridad Informática

3.3 Equipo para la Gestión de Incidentes en la Seguridad de la Información.

El equipo de personas está situado bajo la Subdirección en Seguridad de la Información, el equipo está integrado por tres especialistas en el ámbito de la seguridad de la información cubriendo un horario de atención los veinticuatro horas del día, los siete días de la semana, los trescientos sesenta y cinco días del año, siendo responsable de las siguientes actividades:

- Evaluación inicial de un evento o incidente de seguridad de la información mediante un análisis de riesgo.
- Determinar los servicios o personas adicionales que deben participar en la gestión y resolución del Incidente.
- Centralizar el procedimiento de respuesta ante los incidentes de información para asegurar la rápida y la mejor gestión de los mismos.
- Garantizar el cumplimiento del artículo 316 Bis 12, Fracción I y II, Capítulo X, Sección Cuarta de la Ley de la Comisión Nacional Bancaria y de Valores correspondiente al uso del servicio de la

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

Banca Electrónica que refiere la seguridad, confidencialidad e integridad de la información transmitida, almacenada o procesada a través de Medios Electrónicos. (*Apéndice 1*)

- Investigar de manera rápida y oportuna la evaluación de los incidentes de acuerdo al modelo de riesgo de la Institución basado en la cantidad de información expuesta, el impacto financiero, el daño al prestigio y el posible cumplimiento a leyes regulatorias para asegurar que todos los riesgos identificados sean medidos y controlados con el fin de lograr la oportuna y correcta evaluación de los incidentes por nivel de riesgo con el fin de mitigar, evitar, transferir o asumir el riesgo.

- Se encarga del seguimiento y reporte de los incidentes.

- Identificar vulnerabilidades / amenazas en las políticas, sistemas y procesos que se puedan presentar.

Es oportuno manifestar que para los casos en los que un incidente ocurre a causa de una debilidad en una política o un proceso, el equipo para la gestión de Incidentes en la Seguridad de la Información trabajará con las Direcciones indicadas para detectar la causa raíz del incidente y trabajar en una parte de remediación de la misma para evitar que incidentes similares vuelvan a ocurrir.

El equipo para la Gestión de Incidentes en la Seguridad de la Información tiene como punto de contacto una cuenta genérica de correo electrónico, la cual es monitoreada los trescientos sesenta y cinco días del año, también cuenta con equipos de telefonía celular habilitados con mecanismos de control de acceso para contar con una capacidad de respuesta menor a quince minutos por reporte dependiendo de la condición crítica del incidente con el objetivo de mitigar los efectos de los problemas relacionados con la Seguridad Informática.

Una de las actividades de mayor valor para la Institución es la capacitación que imparte el equipo para la gestión de incidentes en la Seguridad de la Información, en donde se da a conocer a la mayoría de los empleados los temas que involucran la integridad, confidencialidad y autenticidad de la información, el ciclo de vida de la información, el proceso de atención en cuanto al manejo de incidentes y el canal de comunicación. Por último, el equipo para la Gestión de Incidentes en la Seguridad de la Información se encarga de establecer acuerdos de trabajo y niveles de servicio en todas las áreas de la Institución que involucran a las Tecnologías de la Información en la Institución.

(1) *Apéndice. Art 316 Bis 12, Fracción I y II, Capítulo X, Sección Cuarta de la Ley de la Comisión Nacional Bancaria y de Valores*

3.4 Toma de la Función.

En Julio del 2010 comencé a laborar en un Institución Financiera en la Subdirección de Seguridad Informática, en la cual formé parte de un equipo enfocado a la protección de los activos informáticos y el manejo de los posibles Incidentes que afecten los tres de los cinco servicios de seguridad contenidos en el estándar ISO 7498-2: integridad, confidencialidad y autenticidad dejando fuera de este proyecto la disponibilidad y el no repudio ; en específico para continuar con la operación de un programa previamente existente llamado “Atención de Incidentes Informáticos” creado por la Institución para brindar un servicio interno con el objetivo principal de administrar y coordinar las vulnerabilidades y amenazas en la seguridad de los activos informáticos dentro de la Institución financiera, siendo este programa una guía para el manejo de Incidentes en la Seguridad de la Información operado por un empleado ubicado dentro de la Dirección General de Fraudes, a que continuación se describen las seis etapas del programa All

- 1 Notificación: Todos los posibles Incidentes en Seguridad de la Información deberán reportarse con los requisitos que se establecen dentro del marco normativo de las políticas internas en seguridad de la Institución como lo son: el qué, cómo, cuándo y dónde a la cuenta de correo institucional seguridad_TI@dominio.com.mx; una vez que los casos eran reportados la antigua administración comenzaba con la atención del caso.
- 2 Investigación y seguimiento: Cuando ocurría algún caso este era evaluado con forme al siguiente criterio: al presentarse un reporte relacionado a una violación de una política de la institución el caso era clasificado como un evento, al presentarse un caso en donde aunado a la violación de una política se identificaba compromiso de información, este se clasificaba como un incidente en la seguridad de la información y al tener un reporte sin estar ligado a ninguna de las dos anteriores clasificaciones, este quedaba registrado como un Falso Positivo. El empleado encargado de operar el programa registraba los detalles en una aplicación Institucional para el seguimiento de las notificaciones, la cual se utilizaba para llevar un control de los falsos positivos, eventos e incidentes, sin generar informes, métricas y sin proporcionar información que ayudará a obtener un análisis causa-raíz. Con base al programa All, los reportes de seguridad se clasificaban bajo una de las siete categorías que establece el programa de la Institución Financiera de la siguiente manera:
 - Información contenida en Equipos de Cómputo perdidos o robados; ejemplo: una computadora portátil, teléfonos móviles institucionales con servicio de datos y discos duros.

(1) ISO 7498-2 Arquitectura de Seguridad.

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

- Información contenida en documentos físicos o electrónicos perdidos, robados o información comprometida; ejemplo: toda notificación en donde la información física o electrónica que se viera comprometida, esto dependía de la clasificación de la información de la Institución.
- Información que se veía comprometida cuando una persona logra obtener acceso sin autorización a un sistema, aplicación o datos.
- Información que se veía comprometida cuando una persona teniendo legítimo acceso a un sistema, aplicación o información la utiliza de forma en que la exposición de ésta resulte en un daño para la institución o sus clientes.
- Información que se veía comprometida mediante ataques electrónicos dirigidos a la Institución o nuestros clientes como infecciones de malware y denegación de servicio.
- Información que se veía comprometida mediante la persuasión, engaño o manipulación para obtener información por medios no técnicos ilícitos de los empleados.
- Phishing es un intento de obtener información confidencial de los clientes mediante el engaño o la manipulación utilizando medios electrónicos, principalmente el correo electrónico

Dependiendo de la criticidad del incidente, para casos graves acorde a operación y con base en el criterio del empleado a cargo de la misma se acudía a la Alta Dirección con el fin de obtener los pasos para contener el incidente. Los incidentes se podían reportar a la administración de Planeación de Continuidad del Negocio (BCP) para evaluar si se necesitaba una mayor participación de este equipo.



Figura 3.2 Categorías del Programa All

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

- 3 Evaluación del Riesgo: Ésta etapa se realizaba mediante un análisis cualitativo con base en la exposición de la información, impacto financiero e impacto a la reputación de la Institución, dependiendo de la combinación de los tres aspectos mencionados anteriormente con forme la metodología cualitativa institucional para medir el riesgo se obtenía como resultado tres posibles niveles de riesgo como lo son:
 - Nivel de Riesgo Bajo.
 - Nivel de Riesgo Medio.
 - Nivel de Riesgo Alto.

- 4 Ejecución de un Plan de Remediación: Esta etapa dependía de la evaluación del riesgo, en donde se coordinaban acciones para establecer controles compensatorios y/o proteger la información expuesta relacionada al reporte dependiendo de la categoría y clasificación del mismo.

- 5 Validación de la Resolución del evento / incidente: Esta etapa consistía en darle seguimiento a los casos hasta validar que las acciones coordinadas en la etapa anterior fuesen realizadas exitosamente, teniendo por prioridad minimizar el tiempo de vida del reporte con el fin de no tener reportes abiertos por más de un mes acorde a la antigua administración.

- 6 Documentación del Riesgo y Cierre del Caso: Esta etapa empezaba desde que se recibía la notificación, en donde el empleado a cargo de la operación del programa documentaba cronológicamente todas las acciones tomadas hasta cerrar el caso.

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.



Figura 3.3 Etapas en el proceso de Atención a Eventos /Incidentes

Cada reporte dentro de la primera etapa del programa All, era recibido en una cuenta genérica de correo electrónico y evaluado por el empleado encargado de este proyecto en el 2010 ubicado dentro de la Administración de Fraudes Informáticos, la evaluación la realizaba mediante un análisis de riesgo cualitativo con base a la metodología de riesgos institucional mencionada en la etapa tres del programa, el resultado de este análisis hecho con una aplicación institucional segmentaba los reportes dependiendo su nivel de riesgo en tres clasificaciones, las cuales son las siguientes:

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

Falsos Positivos: Eran cualquier caso en donde no existía un compromiso de información manejada, almacenada y distribuida por la Institución.

Evento en la Seguridad de la Información: Se clasificaban como aquellos casos en donde como resultado de una investigación y un análisis de riesgo hecho por los especialistas se identificaba una violación a una política dentro del marco normativo dando como resultado un nivel de riesgo bajo para la Institución, sus clientes y las partes relacionadas. De lo anterior era poco probable que el evento dé como resultado una acción legal o regulatoria, una pérdida financiera o un daño para la Institución, sus clientes o las partes relacionadas.

Incidente en la Seguridad de la Información: Se clasificaban aquellos casos en donde el resultado de una investigación y un análisis de riesgo hechos con la aplicación institucional se obtenía como resultado de la etapa dos y tres del programa un riesgo medio o alto para la Institución, sus clientes y las partes relacionadas con con forme la metodología cualitativa institucional para medir el riesgo; por ello era necesario tomar acciones inmediatas, acciones secundarias, recolectar evidencia y tomar medidas correctivas para disminuir las consecuencias del mismo. En algunos casos era probable que el Incidente resultara en una acción legal o en un cumplimiento regulatorio, pérdida financiera o daño para la Institución, sus clientes y las partes relacionadas. Los Incidentes de información no sucedían de manera frecuente.

Laborando al filo de dos semanas en la institución financiera leí toda la documentación referente al programa All, pudiendo visualizar el alcance y progreso del mismo encontrando que no se logró tener los resultados establecidos durante el periodo Mayo del 2009 – Junio del 2010, como lo fueron:

- Lista actualizada de contactos por cada Administración de TI.
- Diagramas de flujo por cada etapa del programa All.
- Acuerdo de trabajo por cada Administración de TI
- Nivele de servicio por cada Administración de TI con base a niveles de riesgo.
- Evidencia de pruebas con la Administración de BCP.
- Capacidad de identificar un incidente en la seguridad de la información
- Capacidad de respuesta ante un incidente en la seguridad de la información.
- Elaborar reporte ejecutivos.

Así como lograr, que los empleados conozcan que se puede reportar y los medios para hacerlo, ya que por diversos factores ajenos a este escrito la operación del programa se encontraba a cargo un empleado que no tenía la formación académica de un Ingeniero en Cómputo o una carrera a fin

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

como por ejemplo, Licenciado en Informática, etc. para llevar las actividades correspondientes que además dividía su tiempo en este y otros proyectos, lo cual dio como resultado que no se cumplieran correctamente los lineamientos establecidos para este programa ya que no se daba un correcto seguimiento al reporte, no existiendo registros del manejo del reporte en la herramienta Institucional, ni datos que junto con mi nuevo equipo nos ayudaran a conocer la causa raíz del reporte, por lo que no se podían tener información relacionada con tiempos de vida y atención por cada reporte recibido, ni un control de seguimiento que nos pudiera dar detalles de los casos atendidos.

3.5 Problemática y Necesidades.

Actualmente todas las empresas que manejan información sensible están expuestas a sufrir una brecha en la seguridad de la información, la cual puede tener el potencial de causar un extensivo daño a una institución, sus clientes y entidades relacionadas. Se puede definir una brecha en la seguridad de la información como una afectación en la confidencialidad, integridad y autenticidad de la información como por ejemplo, la presencia de un virus⁽¹⁾ u otro "mal-ware"⁽²⁾ en máquinas conectadas en la red de la empresa, una actividad de red sospechosa e inexplicable, pérdida de la confidencialidad en información previamente clasificada como confidencial, la destrucción no autorizada de los datos, la pérdida de la integridad de información en sistemas, aplicaciones y documentos, una negación de servicios, la pérdida de la integridad de los datos, el uso no autorizado de los recursos de empresa, etc.

La mayoría de las violaciones a la seguridad de la información en los últimos años pueden atribuirse directamente al comportamiento de los empleados, ya sea por descuido ó una actividad maliciosa, por lo que bajo estos antecedentes es fundamental contar con un Equipo para la gestión de Incidentes en la seguridad de la Información teniendo como objetivo salvaguardar tres de los cinco servicios de Seguridad (Integridad, Confidencialidad y Autenticidad) contenidos en el ISO 7498-2, enfocados a velar por el negocio y todos los aspectos que lo rodean.

Actualmente en las grandes Instituciones Financieras el tema seguridad de la información ha cobrado mucha fuerza y como resultado en algunas empresas se han creado Áreas/Gerencias/Direcciones teniendo como objetivo impulsar el negocio brindando protección a los activos informáticos. Contar con un Equipo para la gestión de Incidentes no sirve de nada si éste no cuenta con el apoyo necesario de la alta dirección para desarrollar la función de gestión de riesgos en la información.

(1) Virus: malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario

(2) Malware: Código malicioso diseñado para dañar o hacer o realizar acciones no autorizadas en un sistema informático.

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

Como parte de la evaluación que efectué al programa existente para la gestión de los incidentes en la seguridad de la información, encontré que la operación no cumplió con requerimiento mínimos que desde mi punto de vista son necesarios para operar el programa ya que no se brindaba un buen servicio derivado de quejas con respecto al programa All por parte de algunos empleados debido a la falta de apego al programa, calidad en el servicio brindado y seguimiento por parte del equipo laboral que se encargaba de su operación, por ello la mayor parte de los empleados en la Institución Financiera no tenía conocimiento de la existencia del programa, y como consecuencia de lo anterior, los empleados tenían un gran desconocimiento de qué hacer ante una situación en donde se pusiera en compromiso la integridad, confidencialidad y autenticidad de la información.

El equipo para la gestión de Incidentes en la Seguridad de la Información debe ser capaz de identificar vulnerabilidades mediante análisis de riesgos con respecto a los casos notificados, debe tener bien estructurada y segmentada su función, así como contar con un sistema para el seguimiento de los casos notificados, de igual forma construir una red de contactos específicos en todas las áreas en las Tecnologías de la Información para actuar rápidamente en caso de necesitar la colaboración dentro de las administraciones de los principales Equipos de TI con sus respectivos niveles de servicio, es decir, un rápida atención con base a la criticidad del caso reportado con forme a la etapa tres del programa All como lo son por ejemplo:

- Administración de Antivirus.
- Administración de Servidores de correo.
- Administración de Inventarios de Hardware.
- Administración de Zona Desmilitarizada.
- Administración de Arquitectura de la red.
- Administración de las Aplicaciones.
- Administración de Accesos (Altas/bajas).
- Administración de Bases de datos.
- Administración de Software Institucional.
- Administración de Hardware Institucional.
- Administración de Telecomunicaciones.
- Administración de Evaluaciones de Seguridad a Proveedores.
- Administración de Soporte Técnico.
- Administración del Centro de Atención a Empleados.
- Administración de Seguridad Física.
- Administración Continuidad y Recuperación del Negocio

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

Una vez evaluado el caso e identificadas las Administraciones a involucrar en las Tecnologías de la Información, se deberá desarrollar y coordinar planes de mitigación con respecto a los riesgos identificados y medirlos con base a la etapa tres del programa, la cual tiene como función principal priorizar las acciones a tomar derivadas de los niveles de riesgo basados en la criticidad de la información, es decir, definir cuál es el valor de la información en función de la operación para el negocio, traduciendo el lenguaje técnico a lenguaje ejecutivo para la elaboración de métricas y reportes ejecutivos correspondientes para la alta dirección de la Institución partiendo del siguiente principio “Lo que no se mide, no se puede controlar”.

Se necesita dar a conocer el programa Gestión de Incidentes en la Seguridad de la Información a la mayoría del personal de la Institución, ya que todos los esfuerzos planeados y llevados a cabo no sirven de nada si los empleados no son capacitados/entrenados en el tema, se les debe impartir por ejemplo, una presentación con el fin de crear en ellos una conciencia con respecto al manejo seguro de la información (creación, manejo y destrucción) y cómo actuar ante una situación en la que se sospeche un incidente en la seguridad de la información como por ejemplo: recibir un correo Spam⁽³⁾, Phishing⁽⁴⁾, algún código malicioso, pérdida de un equipo de cómputo que contenga información clasificada como confidencial, acceso no autorizados a programas, servidores y sistemas o aplicaciones.

3.6 Inventario de los procesos.

Realicé un análisis de todos los archivos y documentación existente con el fin de evaluar la actual situación del programa, buscando los elementos esenciales a efecto de continuar con la operación del mismo, así como contar con los elementos necesarios con el fin de estar preparado para tener una correcta gestión de Eventos/Incidentes en la Seguridad de la Información cuando éstos llegasen a presentarse. Cuando realicé el inventario de los procesos, encontré puntos clave a mejorar en cada etapa del programa como lo fue en la primera etapa el proceso de notificación de eventos/incidentes en la seguridad de la información ya que, no se contaba con un documento en donde se especificara la forma de reportar un caso, los requerimientos necesarios e información necesaria para comenzar con la atención de la notificación, ¿a qué departamento?, ¿a que área?, cuenta de correo electrónico o número telefónico en donde se envíen las notificaciones, cuáles son los casos que se pueden reportar, tiempos de atención y nivel de servicio para con las notificaciones así como los responsables de la operación.

(3) Spam: Correo no deseado.

(4) Phishing: Intento de obtener información confidencial de los clientes mediante el engaño o la manipulación utilizando medios electrónicos, principalmente el correo electrónico

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

El Programa All contaba únicamente con el manual de operación genérico de la Institución Financiera al cual contiene junto con mi equipo de trabajo propusimos agregar requerimientos a seguir durante y después de recibir una notificación de un Evento/Incidente, mismos que a continuación se detallan en cada etapa del programa:

1.- Compartir la mayor cantidad de información posible.

Una vez que era recibida una notificación a la cuenta de correo seguridad.IT@dominio.com.mx, se tenía que realizar un resumen del caso para determinar qué administración era la involucrada para la coordinar la gestión del Evento/Incidente. Si se requería mayor información, se le pedía al usuario que reportó el problema un mayor detalle de su previa notificación mediante llamadas telefónicas.

2.- Evaluación del riesgo.

La primera valoración del riesgo era llevada a cabo por el Equipo para la Gestión de Eventos/Incidentes tomando en cuenta el número de registros expuestos/comprometidos, un posible impacto financiero, un posible impacto en la reputación y la posible necesidad de un cumplimiento a una ley regulatoria.

3.- Confirmación del nivel de Riesgo.

Una vez realizado el resumen del Incidente y una pre-evaluación del riesgo el Equipo para la Gestión de Eventos/Incidentes tenía que validar el nivel de riesgo con la Administración y el Oficial en Seguridad de la Información asignado a la misma, en la cual se originó el incidente de seguridad, así como todos los departamentos de la Institución que hacen uso de la información, con el fin de validar el impacto que tuviese un posible mal uso de la información.

El papel del Oficial de Seguridad es muy importante ya que mediante este, se localizan rápidamente a los involucrados,

4.- Proceso de Mitigación de Riesgo enfocado a Mitigar, Evitar, Trasferir o asumir el Riesgo.

Este proceso radicaba en crear un plan de acciones iniciales para los Incidentes con el objetivo de Mitigar, Evitar, Trasferir o asumir el Riesgo, el cual tenía que ser elaborado y propuesto por el Equipo para la Gestión de Eventos/Incidentes junto con los Oficiales de Seguridad en cada Dirección de la Institución Financiera y una persona de un Equipo Central dependiendo del área o áreas a involucrar. Estos procesos eran dirigidos a los Incidentes clasificados como riesgos Medios y Altos, de igual forma para algunos Incidentes que requirieran este proceso la realización de una junta para responder al Incidente abordando los siguientes puntos:

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

Tareas a realizar durante el tiempo de vida del Incidente.

- ✓ Confirmación del impacto de la evaluación del riesgo
- ✓ Desarrollo de un plan de acción para la solución del Incidente
- ✓ Actualización del incidente, impacto y acciones tomadas.
- ✓ Determinar los requerimientos del área afectada por el Incidente
- ✓ Y si se requieren notificaciones durante el incidente, desarrollar un plan de comunicación.
- ✓ Si el usuario requiere de notificaciones, desarrollar un plan de comunicación.

5.- Funciones en la etapa del manejo del Incidente.

Una vez culminado el Proceso de Mitigación de Riesgo, la responsabilidad del Equipo para la Gestión de Eventos/Incidentes era la de asegurarse de que todas las acciones a tomar en las etapas previas fueran llevadas a cabo en tiempo y forma, así como informar el proceso del incidente a las áreas involucradas bajo las siguientes acciones:

- ✓ Coordinar juntas para el seguimiento del Incidente en caso de ser necesarias.
- ✓ Confirmar por parte de los encargados de realizar las acciones para mitigar el Incidente, que éstas están siendo realizadas y completadas. (si es necesario)
- ✓ Confirmar con las áreas afectadas y el Oficial de Seguridad de la misma que las acciones a tomar durante el Incidente se están llevando a cabo (si es necesario)
- ✓ Realizar una nueva evaluación del impacto y riesgo en caso de ser necesario.
- ✓ Mantener informado a la alta dirección en caso de ser necesario (para niveles de riesgo Medio y Alto)

6.- Cierre del Incidente.

Una vez que el Equipo para la Gestión de Eventos/Incidentes ha validado el nivel de Riesgo y el plan de mitigación de riesgo se haya realizado, se procedía a identificar las políticas involucradas violadas durante el Incidente, una vez realizado lo anterior, éste se podía cerrar.

El Proceso de Notificación para los Eventos/Incidentes era una parte fundamental en la gestión de los mismos, al momento de que tomé el programa no se contaba con una matriz de contactos por cada una de las siete categorías que marca el programa, únicamente encontré una lista de correos electrónicos y números telefónicos no actualizados sin orden, resaltando que los diagramas de flujo existentes no estaban segmentados por cada una de las seis categorías del programa, además de no estar actualizados.

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

Por lo anterior, validé el mal funcionamiento de los contactos existentes durante la toma de la función, ya que cuando probé cada uno de éstos en dos categorías seleccionadas al azar nunca pude atender una notificación dado que los nombres existentes ya habían dejado el Departamento o la Institución y en adición, el software Institucional para registrar el seguimiento de las notificaciones no fue utilizado desde mi punto de vista con un enfoque Seguridad de la Información ya que los pocos casos registrados no contenían los elementos cronológicos suficientes para realizar un análisis de la notificación con el fin de poder identificar la causa raíz del Incidente y todos los pasos que el antiguo Equipo realizó conforme a la gestión del Incidente.

La antigua administración del Equipo para la Gestión de Eventos/Incidentes en la Seguridad de la Información contaba con acuerdos de trabajo verbales con el área encargada de las tecnologías de la Información; erróneamente y por consecuencia encontré que no existían documentos que avalaran los acuerdos verbales. Un proceso fundamental para realizar una rápida gestión de un Incidente era contar con acuerdos y niveles de servicio documentados, firmados a altos niveles, ser probados con periodicidad, actualizados y tener cláusulas de notificaciones escritas en caso de existir cambios de responsables. En adición un punto a resaltar es la existencia de un plan de recuperación y continuidad del negocio bien estructurado enfocado y preparado para escenarios de desastres naturales con la función de poder continuar la operación de la institución financiera, sin embargo el tema Seguridad de la Información por desconocimiento no fue considerado.

Mes con mes dentro de la institución financiera se realizaban juntas laborales dentro de la Dirección General en Seguridad Informática para conocer a detalle los eventos/incidentes que afectaron la Seguridad de la Información durante el mes, de esta forma si es que un Incidente continuaba en estado activo se pudiera verificar el correcto seguimiento del mismo hasta su cierre, la inasistencia a éstas reuniones por parte de las personas que operaban el programa era común debido a la falta de tiempo y/o la falta de eventos/incidentes que reportar. Así mismo, no se generaban Métricas adicionales a los casos totales reportados por cada mes clasificados por Eventos e Incidentes.

Dentro el inventario que realicé, busqué los perfiles de trabajo para cada integrante del Equipo para la Gestión de Incidentes en la Seguridad de la Información siendo este tema de suma importancia para la definición y segmentación de las funciones laborales que cada miembro del Equipo debe realizar, desafortunadamente no los encontré documentados, adicional a la falta de documentación de funciones laborales, los administradores del programa no cumplían un monitoreo 24 x 7, por consecuencia, en caso de presentarse un Incidente o una actividad

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

sospechosa en fines de semana, esta era atendida hasta el principio de la semana aceptando los riesgos que esto implicaba.

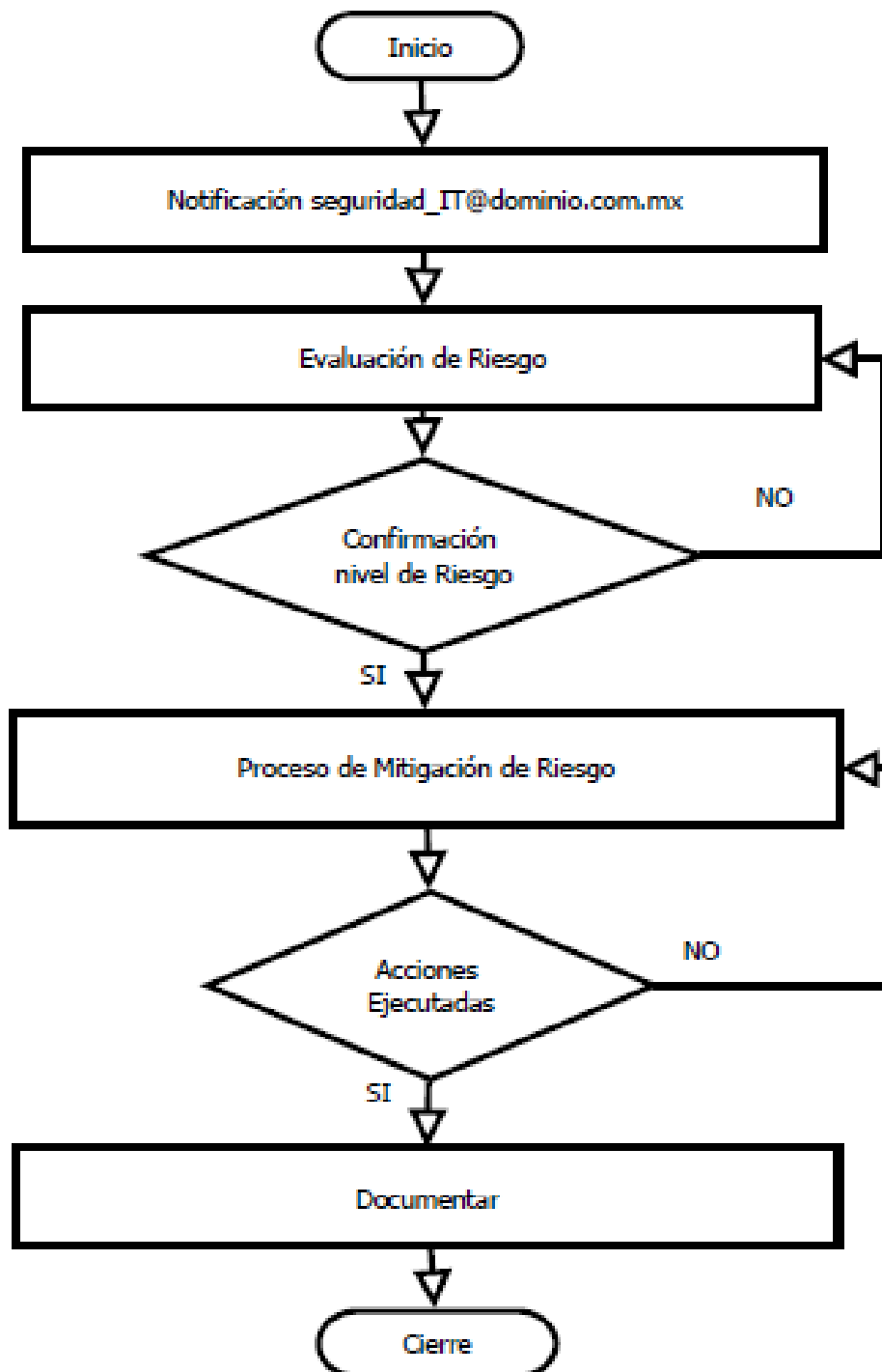


Figura 3.4 Diagrama de flujo del proceso de atención a Eventos/Incidentes

3.7 Campo legal a cubrir.

Las leyes regulatorias siempre son un tema por el que todas las Instituciones Financieras deben estar pendientes para su cumplimiento, cuando ocurre un Incidente en la Seguridad de la Información, durante el proceso de atención del mismo se puede presentar la obligación de realizar una notificación ante las entidades regulatorias del país como parte del proceso de mitigación, como lo indica el marco jurídico de la Comisión Nacional Bancaria y de Valores dentro de las disposiciones de carácter general aplicables a las Instituciones de Crédito, publicada en el Diario Oficial de la Federación el Lunes 5 de julio del 2010 con fundamento en lo dispuesto por el Artículo 52 de la Ley de Instituciones de Crédito, así como por los Artículos 4, fracciones I, XXXVI y XXXVIII y 19 de la Ley de la Comisión Nacional Bancaria y de Valores, dentro de Capítulo X que habla “Del uso del servicio de Banca Electrónica” en su Sección Cuarta “ De la seguridad, confidencialidad e integridad de la información transmitida, almacenada o procesada a través de Medios Electrónicos

Artículo 316 Bis 12.- En caso de que la Información Sensible del Usuario sea extraída, extraviada o las Instituciones supongan o sospechen de algún Incidente que involucre accesos no autorizados a dicha información, deberán:

- I. Enviar por escrito a la Dirección General de la Comisión encargada de su supervisión, dentro de los cinco días naturales siguientes al evento de que se trate, la información que se contiene en el Anexo 64 de las presentes disposiciones.
- II. Llevar a cabo una investigación inmediata para determinar si la información ha sido o puede ser mal utilizada, y en este caso deberán notificar esta situación, en los siguientes 3 días hábiles, a sus usuarios afectados a fin de prevenirlos de los riesgos derivados del mal uso de la información que haya sido extraída, extraviada o comprometida, debiendo informarle las medidas que deberán tomar. Asimismo, deberán enviar a la Dirección General de la Comisión encargada de su supervisión, el resultado de dicha investigación en un plazo no mayor a cinco días naturales posteriores a su conclusión.

Por otra parte, como lo establece el Marco Normativo del Instituto Federal de Acceso a la Información a partir del 12 de junio del 2003, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental obliga a todas las dependencias y entidades del Gobierno Federal a dar acceso a la información contenida en sus documentos respecto, entre otras cosas, a su forma de trabajo, al uso de los recursos públicos, sus resultados y desempeño. La Ley, aprobada en junio del año 2002, es producto de la participación de grupos de la sociedad que llevaron una iniciativa propia del Ejecutivo Federal al Congreso y los legisladores, quienes la aprobaron en forma unánime. Con base en la Ley, fue creado el Instituto Federal de Acceso a la

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

Información Pública (IFAI), un organismo autónomo encargado de garantizar a todas las personas el acceso a la información pública y la protección de sus datos personales que posee el gobierno federal. Por lo que el Equipo para la Gestión de Incidentes en la Seguridad de la Información debe tomar en cuenta los siguientes artículos establecidos por la ley para su cumplimiento:

Atenuación de sanciones.

Artículo 46: En términos de lo dispuesto en el artículo 65, fracción III de la Ley, en los casos en que ocurra una vulneración a la seguridad de los datos personales, el cumplimiento de las recomendaciones que el Instituto emita en materia de medidas de seguridad se tomará en consideración para determinar la atenuación de la sanción que corresponda.

Funciones de seguridad.

Artículo 47: Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien contratar a una persona física o moral para tal fin.

Factores para determinar las medidas de seguridad.

Artículo 48: El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores:

- i. El riesgo inherente por tipo de dato personal;
- ii. La sensibilidad de los datos personales tratados;
- iii. El desarrollo tecnológico, y
- iv. Las posibles consecuencias de una vulneración para los titulares.

De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos:

- v. El número de titulares;
- vi. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento;
- vii. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para un tercero no autorizado para su posesión, y
- viii. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.

Para tales efectos, dentro de las funciones del Equipo para la Gestión de Incidentes en la Seguridad de la Información, esta el comunicar a la Administración de Legal cada incidente en el cual se ve expuesta la información citada en la ley, así como apoyar en la obtención de cualquier evidencia tecnológica requerida para la elaboración del reporte.

3.8 Implementación del programa GISI. (Gestión de Incidentes en la Seguridad de la Información)


Una vez que realicé el inventario de los procesos existentes y leído por completo la documentación de la función, fui capaz de visualizar el alcance que se pretendía, llevando una correcta operación del programa, por lo que una de las primeras tareas que realicé (como parte del equipo de tres personas contratadas), fue mediante un software plasmar las tareas a realizar para alinear la operación diaria a los verdaderos alcances del proyecto, , tareas que fueron priorizadas basadas en la criticidad de su ausencia tomando en cuenta que el programa ya estaba en ambiente de producción al momento en que entré a laborar en la Institución Financiera. Como parte de los primeros cambios realizados fue renombrar el programa Atención de Incidentes Informáticos (AII) a Gestión de Incidentes en la Seguridad de la Información (GISI), esto debido a la mala reputación que el antiguo nombre le daba al programa.

Como primera acción realicé junto con el equipo de trabajo como lo marcó nuestro calendario tal y como lo representa la (Tabla 3.1) fue la definición de funciones laborales para el Equipo de Primera Respuesta para Eventos en la Seguridad de la Información; para este puesto determiné la necesidad de contar con una persona de tiempo completo (ya contratada) que en un futuro pudiese cumplir con una cobertura de monitoreo 24 x 7 para dar cumplimiento a esta función, lógicamente se necesitaba los accesos a las aplicaciones Institucionales para el perfil de la función, un teléfono móvil en el que se puedan recibir las notificaciones, una Lap Top para en caso de ser necesario poder atender una notificación y una BAM para conectarse vía VPN, puntualizando que todos estos requerimientos fueron pedidos a la alta dirección. Parte de esta primera actividad fue determinar los mismos requerimientos para el Equipo de Gestión de Incidentes en la Seguridad de la Información.

Como parte de la toma de la función realicé un inventario de todos los procesos, documentos, acuerdos, y compromisos por parte de la antigua Administración de la Institución, tomando las cosas útiles y desechando todo aquello que no servía como lo fue un control para el seguimiento de las notificaciones, acuerdos con áreas del negocio que obligaban a los antiguos administradores a cumplir con requerimientos ajenos a la función, es decir, deseché actividades ajenas a nuestras funciones laborales y junto con el nuevo equipo comencé a crear nuestra red de contactos con las Administraciones de las Tecnologías de la Información, actualizando esta matriz cada seis meses, así mismo asistí a las juntas convocadas por la Alta Dirección para dar a conocer la función mejorada. Todas las actividades previamente descritas las realicé junto con mi equipo de trabajo mientras atendíamos la operación diaria de la función, es decir, continué con la operación mientras desarrollé el modelo de implementación, obteniendo como resultado ocho puntos de suma importancia divididos cada uno de éstos por un periodo de tiempo.

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

Tabla 3.1 Tareas a desarrollar para la implementación del programa

ID		Task Name
1		Start
2		FRT Definition
3		Personnel Conformation
4		Role definition
5		Personnel contracting (One staff)
6		Personnel contracting (full team)
7		Personnel Training
11		Coverage (24 X 7) Definition
12		Resources (BBs, BAM, etc)
13		Function Take Over
14		Old team running REACT
15		Receiving the Function
16		Review of what is done
17		Take useful & dismiss unuseful
18		Continuing function while new model is implemented (Bridge)
19		Deploy Group IM Model
20		Engauge other Areas - Define Responsibles
21		Enroling BIR0s
22		Enroling LOBs
23		Enroling ITD
24		Enroling ITO
25		Enroling Complementary areas (using BIR0s)
32		Enrole S&F (Find specilists in:)
35		Enrole ISR (Find specilists in:)
43		Train Involved Staff
47		Definitions
48		Classifications
52		IMT Definition
53		Establish IMT Network
54		Define Contact Control
55		Train: IMT contacts in IM process and needs
56		IM Process Operational
57		Migrate to Archer
58		Update Archer
59		Old Manual REACT Process
60		Parallel Controls
61		Archer Stand Alone Process
62		Tracking, Reporting & Control Process: Remeadiation
63		Define raising to GORDON Process
64		Defining raising to BCP Process
65		Establish Lesson Learned Process for Incidents
66		Trend Analysis Process
67		Asosiation with recognized entities & suppliers
68		Enrolling Authorities Process
69		SMEs
70		Identification
71		Enrolling
72		Preventive & Corrective Processes
73		Documentation
74		Gathering Previous documentation
75		Document Take Over Proces
76		Document New Functions
77		Document New Structure
78		Document Arrangements with all parties
79		Implement SLAs for all IMT members
80		Document New Functions

3.9 Acuerdos y niveles de servicio.

No se puede contar con un Equipo para la Gestión de Incidentes en la Seguridad de la información sin tener “brazos” (personal encargado y capacitado) en la dirección de TI que ejecuten las instrucciones previamente analizadas y justificadas con base en un nivel de riesgo, en específico los brazos ejecutores más importantes para la función son las áreas relacionadas con las Tecnologías de la Información y los Oficiales de Seguridad de la Información en cada una de las áreas de:

- Administración de Antivirus.
- Administración de Servidores de correo.
- Administración de Inventarios de Hardware.
- Administración de Zona Desmilitarizada.
- Administración de Arquitectura de la red.
- Administración de las Aplicaciones.
- Administración de Accesos (Altas/bajas).
- Administración de Bases de datos.
- Administración de Software Institucional.
- Administración de Hardware Institucional.
- Administración de Telecomunicaciones.
- Administración de Evaluaciones de Seguridad a Proveedores.
- Continuidad y Recuperación del Negocio.
- Administración de Soporte Técnico.
- Administración del Centro de Atención a Empleados.
- Administración de Seguridad Física.

Para todas y cada una de estas administraciones seleccionadas con base en su importancia para nuestra operación, junto con el nuevo equipo de trabajo coordiné capacitaciones enfocadas a directores por cada una de las administraciones citadas anteriormente en las cuales les mostré el valor del Programa resaltando el papel que cada administración representa para la gestión de los Eventos/Incidentes que afectaban la Seguridad de la Información dependiendo del caso y la categoría de nuestra función.

Cada presentación tenía una duración en promedio de dos horas y que al momento en que terminé de presentar el programa GISI con todas las Administraciones, cité un caso ficticio en el que se requería de su urgente colaboración, mostré y expuse cómo atendí el caso no real desde

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

que me es notificado como lo indica el programa, el análisis que realicé dentro de la primera etapa del programa con la recaudación de toda la información que necesité para determinar un nivel de riesgo señalando la causa raíz del incidente enfatizando los riesgos involucrados, y con esta investigación que realicé y con base a mis conocimientos en Seguridad de la Información coordiné un plan de mitigación de Riesgo en donde en un caso ficticio para cada una de las Administraciones, les resalté la importancia de su participación en donde era urgente contactarlos para ejecutar las instrucciones que les solicité atender los más pronto posible; por lo que de esta forma logré concientizar a la mayoría de las Administraciones en su participación dentro de nuestro proceso de atención para lograr mitigar los riesgos de una forma rápida y minimizando un nivel de afectación cuidando los acuerdos de colaboración y sus niveles de servicio, esta actividad fue realizada durante seis semanas teniendo como objetivo organizar dos reuniones por semana (Septiembre 2010 – Noviembre 2010)

Por mencionar un ejemplo, a la Administración de los Servidores de correo y la Administración de Antivirus, les cité un caso en el cual se necesitaba de su urgente colaboración: bajo el escenario en el que un empleado recibe un correo electrónico de una cuenta desconocida (SPAM), lo abre y da click en una URL contenida en el cuerpo del correo, esta URL lo direccionaba a un sitio que contenía un código malicioso que infecta la máquina sin que el empleado se dé cuenta sino hasta que observara un comportamiento anormal en su equipo, una vez que llegó la notificación a nuestro equipo, solicité información y evalué el caso, determinando enviar a bloquear la dirección de correo SPAM de manera urgente para que nadie en la Institución Financiera pudiese recibir este correo y con el Equipo de Antivirus les notifiqué la urgencia de verificar la salud del equipo, procediendo a desconectar este de la red; por otra parte coordiné un escaneo del equipo en sitio, es decir, que un empleado de este departamento verificó el estado del equipo y en caso de confirmar la infección del mismo, validar si el antivirus con el que cuenta la Institución tenía la firma o se tratase de un ataque de día cero, paralelamente solicité validar la existencia de este virus (ficticio) para conocer cuántos equipos se encontraban infectados y tomar las acciones citadas anteriormente lo más pronto posible.

Con estas capacitaciones logré obtener el apoyo de los presentes, resaltando la importancia de su participación en nuestro proceso de atención, ya que sin ellos las acciones de mitigación dependiendo del caso no serían ejecutadas. Estos puntos tan importantes los logré únicamente con el apoyo de mi líder de proyecto, y la Dirección de Seguridad Informática, quienes estuvieron brindando su apoyo en las dieciséis reuniones llevadas a cabo durante (Septiembre 2010 – Noviembre 2010), y en específico en los casos en que tuve problemas para conseguir los acuerdos en cuanto a nivel de servicio que les solicité a cada una de las Administraciones, ya que muchas de éstas Administraciones conscientes de los posibles riesgos que la Institución Financiera podría

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

enfrentar accedieron a cooperar pero, cuando les solicité un tiempo de respuesta no todos fueron muy sensatos, sin embargo al firmar los acuerdos de colaboración y niveles de servicio a nivel Dirección todos aceptaron.

Los acuerdos de colaboración y niveles de servicio deben desde mi punto de vista ser actualizados cada seis meses, nombrando a la administración involucrada como responsable del acuerdo teniendo al menos tres contactos (primario, secundarios y reserva) para la ejecución de las acciones, con sus respectivas extensiones telefónicas y correos electrónicos por cada administración, esto con el fin de prever futuros problemas relacionados con las bajas de los empleados o cambios de áreas. En total logré obtener acuerdos de servicio con veinticuatro administraciones, niveles de servicio con ocho administraciones críticas para la operación durante dos meses.

3.10 Análisis de Riesgo.

Con el fin de evaluar de manera consistente un riesgo derivado de una afectación a la Integridad, Confidencialidad y Autenticidad de la Información, se utiliza la Metodología Institucional para llevar a cabo el análisis de riesgos la cual es de carácter cualitativo y toma como referencia las siguientes dos metodologías:

- NIST SP 800-30.
- MEHARI

Realizar la evaluación inicial del riesgo basado en un enfoque cualitativo permite estimar el posible nivel de riesgo del Incidente con la información conocida hasta el momento en que se realiza la evaluación. El Equipo para la Gestión de Incidentes en la Seguridad de la Información lleva a cabo esta tarea mediante el valor obtenido de la expectativa de pérdida en cual se basa en la combinación de la matriz institucional de impacto en la reputación social, la matriz institucional de probabilidad/Frecuencia de ocurrencia del Incidente y la matriz institucional de exposición de datos (Información de uso exclusivo para las labores y actividades dentro de la Institución Financiera), mismas a detallar en el siguiente punto,

de esta forma se calcula el nivel de riesgo residual y con base a la información recabada durante la investigación tomando en cuenta los siguientes puntos que son fundamentales para posteriormente validar en cada una de las matrices el impacto, la exposición y la probabilidad de ocurrencia:

(2) NSIT SP 800-30, (3) MEHARI

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

- Atención a nuestros clientes / inconformidad
- La clasificación de la información comprometida.
- El potencial del incidente para dar un cumplimiento a una ley regulatoria.
- El potencial de que el Incidente sea informado a través de los medios de comunicación.
- El potencial de comprometer la confianza institucional en la industria de servicios financieros como un proveedor de los mismos.
- La Probabilidad/Frecuencia en que la información interna, restringido y/o altamente restringida se vea comprometida
- La frecuencia en que Terceros pueden verse involucrados sobre un Incidente en donde información de nuestra Bancara este comprometida,

Cada notificación que recibí, fue investigada hasta conocer los puntos anteriormente descritos, con el fin de proceder a consultar cada una de las matrices para obtener el número de impacto, probabilidad y exposición de acuerdo a los campos descritos en cada una de las matrices, siendo mi responsabilidad el realizar una buena investigación para validar la veracidad de la información ya que ésta es la clave para seleccionar los niveles en cada una de las matrices y poder calcular un nivel de riesgo.

Matriz de Impacto al Prestigio.

El primer componente del nivel de riesgo es la imagen de la Institución, como consecuencia potencial de un Incidente en la Seguridad de la Información y teniendo en cuenta cualquier pérdida financiera para la Institución, sus clientes y terceros autorizados que manejen información de la Institución tales como servicio al cliente, la actitud de los medios de comunicación o el impacto en el personal pueden representar un daño severo a la Institución. La puntuación para este Impacto es la siguiente:

- 1 – Insignificante.
- 2 – Menor.
- 3 – Moderada.
- 4 – Grande.
- 5 – Masivo.

Con base a la información que obtuve durante el proceso de investigación para cada uno de los casos, procedí a realizar el análisis de cualquier Incidente haciendo referencia a las siete columnas

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

de la matriz de impacto representada gráficamente en la (Tabla 3.1) que en la página siguiente se muestra en la determinación de la puntuación de impacto adecuado. En algunos casos más de una columna podía aplicar, por lo que con base en mi investigación y conocimiento del tema hice un juicio equilibrado sobre el impacto global del riesgo teniendo en cuenta todos los aspectos descritos en la matriz como lo son: Servicio al Cliente, Medios de Comunicación, Acciones Regulatorias y Legales, Acciones Criminales y una posible Perdida Financiera.

Tabla 3.2 Matriz de Impacto al prestigio

		IMPACTO					
PUNTUACION		SERVICIO A CLIENTE	ACTITUD EN MEDIOS	ACCION REGULATORIA	ACCION LEGAL	CRIMINAL	PERDIDA DIRECTA
1	INSIGNIFICANTE	X	X	X	X	X	-
2	MENOR	X	X	X	X	X	\$
3	MODERADO	X	X	X	X	X	\$\$
4	GRANDE	X	X	X	X	X	\$\$\$
5	MASIVO	X	X	X	X	X	\$\$\$\$

Matriz de Probabilidad de Ocurrencia.

El segundo componente del nivel de riesgo es la probabilidad/frecuencia de que el riesgo volverá a materializarse o se repita. Para la clasificación del riesgo de un Incidente de la Información, teniendo en cuenta el hecho de que el Incidente ya ha ocurrido, el componente de riesgo se centra en el riesgo de que ocurra un incidente similar o de un incidente específico se repita. La escala de puntuación para la probabilidad es la siguiente:

- 1 – Rara.
- 2 – Improbable.
- 3 – Frecuente.
- 4 – Probable.
- 5 – Esperada.

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

Con base a la información que obtuve durante el proceso de investigación para cada uno de los casos, procedí a realizar un análisis en la Matriz de Probabilidad representada gráficamente en la (Tabla 3.2) mapeando la información que recaudé con los puntos descritos en la matriz como lo son: Factibilidad, Situación Regulatoria y Frecuencia.

Tabla 3.2 Matriz de Probabilidad

PROBABILIDAD				
PUNTUACION		FACTIBILIDAD	SITUACION REGULATORIA	FRECUENCIA
1	RARA	X	X	
2	IMPROBABLE	X	X	
3	FRECUENTE	X	X	
4	PROBABLE	X	X	
5	ESPERADA	X	X	

Matriz de Exposición.

El siguiente paso es considerar la Matriz de exposición relacionada con este riesgo. La medida de la exposición es una escala inversa de la eficacia de los controles pertinentes y acciones de mitigación, La escala de puntuación para la exposición es la siguiente:

- 1 - Menor: Altamente eficaces los controles.
- 2 - Limitada: Eficacia de los controles.
- 3 - Medio: Moderada eficacia de los controles.
- 4 - Importante: Deficiencias significativas en los controles.
- 5 - Principales: Controles ineficaces o mínimos

Una vez más, las siete columnas de la matriz de exposición representada gráficamente en la (Tabla 3.1) deben ser consideradas para realizar el análisis, siendo mi deber efectuar un análisis de su exposición al riesgo y la clasificación de la Información, la puntuación de la exposición se utiliza para determinar el valor de la columna en la tabla de evaluación de riesgos. Los resultados

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

de la exposición aumentan con base a la información que obtuve durante el proceso de investigación para cada uno de los casos, procediendo a realizar un análisis en la Matriz de Impacto mapeando la información que recaudé con los puntos descritos en la matriz como lo son: Definición, Diseño de Procedimientos, Diseño de Controles, Mitigación Externa y Efectividad Operativa.

Tabla 3.3 Matriz de Exposición.

EXPOSICION									
EXPOSICION	DEFINICION	DISEÑO DE PROCEDIMIENTOS Y PRUEBAS	EFFECTIVIDAD OPERATIVA	NIVEL DE ACTIVIDAD DE CAMBIO	DISEÑO DE CONTROLES	CLIENTE / CONTRAPARTE	CONTINGENCIA	MITIGACION EXTERNA	
1	MENOR	X	X	X	X	X	X	X	X
2	LIMITADA	X	X	X	X	X	X	X	X
3	MEDIA	X	X	X	X	X	X	X	X
4	SIGNIFICATIVA	X	X	X	X	X	X	X	X
5	GRAVE	X	X	X	X	X	X	X	X

Una vez realizado mi análisis en cada una de las tres matrices, siempre que un Incidente en la Seguridad de la Información se presenta y teniendo en cuenta que no todos los puntos mapeados del Incidente pueden ser iguales en las situaciones descritas en la puntuación de cada una de las matrices, seleccioné de acuerdo a mis conocimientos, situación e investigación del Incidente y posibles consecuencias el número de la puntuación que más se asemejó a la situación a evaluar.

Matriz de Probabilidad (1, 2,3,4,5) = P

Matriz de Impacto (1,2,3,4,5) = I

Matriz de Exposición (1,2,3,4,5) = E

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

Nivel de Riesgo Residual.

Después de evaluar tanto el impacto y la probabilidad del evento de riesgo, los dos resultados se multiplican entre sí para dar la puntuación de riesgo absoluto o residual, tanto la probabilidad y el impacto se miden del 1 al 5, la puntuación máxima absoluta o inherente es 25 y el mínimo es 1. La puntuación se utiliza para determinar qué fila en la tabla de evaluación de riesgos es relevante.

El riesgo residual creado por un incidente representa su nivel global de la vulnerabilidad al riesgo. Esto se determina en referencia a una tabla de evaluación de riesgo. Después de evaluar tanto el impacto y la probabilidad del evento de riesgo, la puntuación de riesgo residual se leerá a partir de la tabla, utilizando el nivel absoluto o inherente del riesgo para determinar la fila y la puntuación de la exposición para determinar la columna.

El cálculo de este riesgo residual se basa tomando en cuenta dos factores anteriores resultado del análisis hechos en la Matriz de Probabilidad y la Matriz de Impacto, con éstos factores se visualiza el impacto potencial del riesgo absoluto o inherente.

$$\text{Nivel de Riesgo Residual} = (\text{Probabilidad}) \times (\text{Impacto})$$

$$\text{Nivel de Riesgo Residual} = (P) \times (I) = Z$$

Z → puede tomar valores entre uno y veinticinco.

El cálculo del nivel de riesgo lo realicé utilizando “Z” y el resultado de la Matriz de Exposición, una vez contando con estos datos únicamente se evalúan en la Tabla de Nivel de Riesgo como se muestra en la (Figura 3.4).

Valor Z	Valor Matriz de Exposición				
	1	2	3	4	5
>10	C	B	B	A	A
>8	C	C	B	B	A
>6	C	C	C	B	B
>4	D	C	C	C	B
>2	D	D	C	C	C

Figura 3.5 Matriz de Nivel de Riesgo

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

- D → Nivel de Riesgo Bajo
- C → Nivel de Riesgo Medio
- B → Nivel de Riesgo Mayor
- A → Nivel de Riesgo Alto

Gracias a la ayuda de un software Institucional realicé y continuo realizando los análisis en cuanto a los posibles niveles de riesgo para la mayoría de las notificaciones que recibimos, este software es de gran apoyo únicamente para realizar el cálculo descrito anteriormente con las matrices como se observa en la (Figura 3.5) ya que la parte de la investigación es fundamental para obtener un nivel de riesgo acorde a la información previamente recaudada.

What is the category of the event or incident?
Is this event or incident internal or third party related?
Has Customer/Consumer/Employee information been exposed? If so, how many records/accounts?
Has (or is it possible that) confidential information been exposed?
What is the financial impact?
What is the reputational impact?
<u>Bermuda</u>
Are any systems impacted or breached?
What is the preliminary risk rating?

Figura 3.6 Software para el cálculo del nivel de Riesgo.

Como miembro del Equipo para la de Gestión de Incidentes en la Seguridad de la Información fue mi deber de acuerdo al resultado del nivel de riesgo convocar una reunión durante toda la vida de un Incidente identificado con un nivel de riesgo, de riesgo medio y alto para asegurar que todas las acciones que coordiné se realizaran en tiempo. Solo para algunos Incidentes clasificados con un nivel de riesgo bajo se puede requerir una reunión con el fin de responder adecuadamente a las cuestiones involucradas en el Incidente.

3.11 META del Riesgo.

Como lo indica el Programa GISI, todos los Eventos/Incidentes que afectan la seguridad de la información deben ser evaluados conforme lo establece la función con un análisis de riesgos; como resultado del análisis se identifican las partes involucradas para participar en la gestión de los mismos, esto con el objetivo de Mitigar, Evitar, Trasferir o Asumir los Riesgos Identificados.

➤ **Mitigación del Riesgo.**

Está enfocada a disminuir rápidamente la gravedad de un Incidente, una vez que determiné el nivel de riesgo de un incidente, mi función era la de coordinar la primera acción basada en un análisis de vulnerabilidades a los procesos, sistemas, aplicaciones y personal involucrado; como resultado del análisis anterior, determinaba acciones a ejecutar ya sea en los procesos, aplicaciones, sistemas o el personal involucrado que dieron origen al incidente. Generalmente es la primera acción que determinaba ejecutar para contener el Incidente.

➤ **Evitar el Riesgo.**

No necesariamente es una acción a coordinar durante el tiempo de vida de un incidente ya que el Equipo para la Gestión de Incidentes en la Seguridad de la Información al realizar un análisis de vulnerabilidades identifica riesgos que aún no dan como origen Incidentes en la Seguridad de la Información, de esta forma el equipo trataba de evitar que la Vulnerabilidad fuera explotada por una Amenaza y se conviertan en un riesgo, por lo que cuando el riesgo es muy probable de materializarse y además no se cuenta con los controles adecuados para minimizarlo o mitigarlo, se decide buscar otra forma o camino para darle continuidad al proceso/función requerida.

➤ **Aceptar el Riesgo.**

No en todas las ocasiones los riesgos identificados pueden ser mitigados, ya que en algunos incidentes las acciones a ejecutar pueden ser más costosas que la combinación del posible impacto financiero y el posible impacto/criticidad del activo a proteger, derivado de un análisis costo-beneficio realizado por el dueño de la Información y avalado por parte del negocio, dentro de este escenario en algunas ocasiones el negocio puede decidir si es más rentable asumir el riesgo que la inversión propuesta para mitigarlo. Es aquí cuando la Dirección de Riesgos en la Seguridad de la Información pide al negocio firmar una carta de aceptación de riesgo.

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

➤ Trasferir el Riesgo.

Derivado de la estructura de la Institución Financiera en algunas acciones es más rentable para el negocio contratar el servicio de un tercero para llevar a cabo ciertas actividades necesarias para la operación del negocio, al realizar esas tareas el tercero tendrá dentro de sus funciones el Información de la Institución, por lo que en específico para estos casos se realizan los contratos de confidencialidad con los proveedores previamente autorizados mediante un proceso de selección. En caso de presentarse una afectación a la información de la Institución manejada por el tercero, este será el responsable de responder por los posibles daños ocasionados.

3.12 Grado de difusión.

Como parte del las tareas a realizar dentro de este proyecto, junto con mi equipo de trabajo y derivado del análisis que le realicé a la función, como resultado encontré un punto muy importante a mejorar, siendo este el desconocimiento del programa ahora llamado Equipo para la Gestión de Incidentes en la Seguridad de la Información ya que para la gran mayoría de los empleados en todas y cada una de las sedes de la Institución casi nadie tenía conocimiento de lo que era este programa, para que servía, Qué reportar? Dónde reportar, Cómo hacerlo? etc.; como parte de la estrategia que junto con mi equipo de trabajo desarrollé para atacar este punto fue el cambio del nombre, con esto propuse realizar el cambio a la cuenta de correo en donde se recibirían posteriormente éstos reportes a una nueva cuenta que tuviera una relación con el nuevo nombre de la Función Equipo para la Gestión de Incidentes en la Seguridad de la Información.


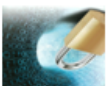
Una vez que fueron atendidos éstos requerimientos junto con mi equipo de trabajo me di a la tarea de coordinar reuniones con las Administraciones pertenecientes a Tecnologías de la Información como es citado en el capítulo 3.6, siguiendo el calendario de actividades que desarrollé junto con mi equipo de trabajo (ver tabla 3.1), convoqué a una reunión con el Comité de Decisión que es integrado por al menos un representante de cada una de las Direcciones del Negocio, en esta reunión les expuse el propósito de nuestra función y su papel como representantes de su Dirección.

Parte de las actividades (ver tabla 3.1) que desarrollé para la difusión del programa GISI fue reunirme con las Direcciones Generales de la institución con el objetivo que la mayoría de sus empleados conociera la función que desarrollamos, donde primero que nada les expuse a la Subdirección de los Oficiales de Seguridad en cada una sus las ocho direcciones una presentación en donde les compartí una breve introducción en cuanto a Incidentes en la Seguridad de la Información, la historia del Programa y cómo evoluciona a Equipo para la Gestión de Incidentes en la Seguridad de la Información, Qué hace y Cuáles son los objetivos de este, les mostré todos los

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

aspectos relacionados a lo que significa un manejo seguro de la información dentro del nuevo Equipo, en donde enfatice el objetivo de nuestra función y Qué se puede reportar? Dónde puedo dirigir mi reporte y Cómo hacerlo?; junto con nuestro proceso de atención en el cuál en cada una de las presentaciones que realicé a los Oficiales de seguridad les cité ejemplos en cada una de las siete categorías como lo marca nuestra función en un posible compromiso en la Integridad, Autenticidad y confidencialidad de la Información. Recalcando que la función que realiza el equipo es Centralizar el procedimiento de respuesta ante los posibles Eventos/Incidentes que afecten la seguridad de la Información para asegurar la rápida y mejor gestión de los mismos, aplicando las mejores prácticas y garantizando el cumplimiento de las regulaciones.

Después de que capacité a los oficiales de Seguridad en cada una de sus ocho Direcciones realicé la misma actividad con su red de Sub-Oficiales de seguridad, y empleados de la Institución Financiera siendo esta presentación vía videoconferencia para cubrir todo el territorio nacional y presencial en las distintas sedes en el Distrito Federal. Para cada una de las cincuenta y cuatro presentaciones realizadas, durante el comienzo de las mismas elaboré una minuta de asistencia que se observa en la (Figura 3.2) con el objetivo de llevar un control por cada una de las Administraciones del Negocio, de esta forma pude medir mes con mes el progreso del personal capacitado, registrando una capacitación por semana con al menos 20 empleados durante más de un año comenzando desde Octubre 2010 a Diciembre 2011 con un total de mil empleados entrenados.

	Equipo para la Gestión de Incidentes en la Seguridad de la Información	
Fecha		Lista de Asistencia
Hora		
Lugar		
		Capactación GISI

Nombre	Puesto	Correo	EXT	Dirección	Firma

Figura 3.7 Minuta de Asistencia a Capacitaciones GISI

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

Por último junto con el apoyo de mi Subdirección logré que por parte de la Alta Dirección se enviara un comunicado a todos los empleados de la Institución Financiera en donde se mencionó que dentro de nuestra Intranet debían visitar el proyecto, en donde se incluyó la presentación que expuse anteriormente a los empleados, con preguntas y conceptos básicos del proyecto como por ejemplo ¿Qué hacer ante cualquier situación en donde se viera comprometida la Integridad, Autenticidad y Confidencialidad de la Información?, siendo los miembros del Equipo encargados de difundir las actividades a realizar, como parte de la firma de nuestro correo incluimos la liga de la Intranet cada al contestar un correo electrónico.

En adición, una vez que el Equipo tuvo ejecutó las tareas propuestas (ver tabla 3.1), coordiné la capacitación de la programa al personal de Seguridad Informática de la Institución Financiera encargado de implementar el Equipo para la Gestión de Incidentes en la Seguridad de la Información con sede en Latinoamérica y Centroamérica, siendo México el primer país en desarrollar este cambio.

3.13 Equipo de primera respuesta para Eventos en la Seguridad de la información.

Una vez que junto con mi equipo de trabajo me encargué del programa, propuse realizar un cambio en cuanto a todo lo relacionado con el nombre de la función, ya que derivado de las charlas que tuvimos con las distintas Administraciones de la Institución Financiera, los oficiales de Seguridad en cada administración del negocio y la capacitación a los empleados, me di cuenta que los pocos que conocían la función tuvieron malas experiencias al reportar algún caso con la antigua Administración. Con base en estos resultados propuse junto con mi equipo de trabajo cambiar la cuenta de correo en donde se recibían anteriormente los casos por una nueva cuenta de correo ahora nombrada GISI@dominio.com.mx la cual se pudiera identificar rápidamente con el nuevo nombre del programa “Equipo para la Gestión de Incidentes en la Seguridad de la Información” – GISI, en donde el equipo de primera respuesta analiza únicamente los eventos en la seguridad de la Información.

El Equipo de Primera Respuesta para los Eventos en la Seguridad de la Información tiene como funciones las siguientes tareas:

- Cumplir con un tiempo de atención, es decir, contestar vía correo electrónico todas las notificaciones que recibíamos en la cuenta de correo GISI@dominio.com.mx con un tiempo máximo de 15 minutos;

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

- Analizar el reporte con base a la etapa dos del programa, dependiendo de la notificación se tomaban acciones para los falsos positivos y para los eventos llevando a cabo un primer análisis de la notificación independientemente de la categoría.
- Registrar todos los detalles del caso en el software Institucional y en la bitácora creada para obtener métricas de todo lo que fue atendido.
- Una vez realizado el análisis seguía el proceso de atención como lo establece el programa, canalizando en caso de presentarse lo incidentes al siguiente nivel.

En general este equipo se encargaba de tomar acciones de mitigación para todos los eventos en la Seguridad de la Información, llevaba un registro detallado haciendo uso del software Institucional y el control interno del GISI para el seguimiento de los eventos, enfatizando que todos los eventos tienen un nivel de riesgo bajo, que en su mayoría los son:

- Phishing.
- Spam.
- Estafas Nigerianas (419)
- Robo de Hardware sin compromiso de información.
- Envío de notificaciones de violaciones de políticas.
- Recaudación de información para la elaboración de Métricas.

Así mismo, este equipo se encargaba además de darle seguimiento a todos los casos, dar una retroalimentación a quienes enviaban las notificaciones, resolviendo dudas que los empleados tenían respecto al antiguo Programa– ahora GISI con el fin de brindar un buen servicio a todos los aquellos que enviaban sus reportes. Este equipo era guiado por el equipo encargado de gestionar los Incidentes, ya que durante el primer análisis hecho en cada caso, cuando se validaba el compromiso de información, el equipo de primera respuesta procedía a canalizar el incidente con el equipo encargado de gestionar los mismos.

3.14 Equipo para la Gestión de Incidentes en la Seguridad de la información.

Como parte de los cambios que realicé, estuvo el proponer que el programa GISI cumpliera como función primordial apegarse manual, el cual básicamente es la versión del antiguo programa, ahora con la única función de atender incidentes, en específico, elaboré un nuevo proceso para la atención de incidentes tomando las siguientes mejoras descritas a continuación:

1.- Compartir información.

Por cada Incidente que recibía, realizaba un resumen de la notificación para determinar qué Administración por parte de la Institución tenía que ser involucrada. Como parte del proceso, en caso de requerir mayor información mi deber era solicitarle al empleado, la información necesaria para realizar el análisis de riesgo respectivo, esta tarea la realizaba elaborando formatos de notificación y textos con los datos indispensables para agilizar esta primera etapa durante el incidente.

2.- Evaluación del riesgo.

La primera valoración del riesgo era llevada a cabo por mí como parte del Equipo para la Gestión de Incidentes en la Seguridad de la Información, en donde una de las mejoras que realicé fue la propuesta de un listado de información a efecto de conocer todos los detalles del caso por cada categoría de la función, para realizar un análisis cuantitativo usando el modelo operacional del grupo previamente descrito, enfocado a obtener los valores numéricos con base al impacto financiero y cantidad de información comprometida; adicional al antiguo proceso de evaluación referido, tomé en cuenta nuevos aspectos de gran importancia durante el tiempo de vida de un incidente, como lo son:

- Identificar y notificar los riesgos del Negocio.
- Concentrar los detalles de los Incidentes para establecer una evaluación preliminar de las afectaciones.
- Estar preparado para declarar una situación de emergencia ante un desastre.
- Coordinar y administrar un plan de recuperación mientras prevalezca la situación de emergencia desde un centro de mando alternativo.
- Establecer los canales de comunicación durante la situación de emergencia.

3.- Notificar al Comité de Decisión

Una vez que realizaba una pre-evaluación de los riesgos sobre un incidente y documentar los detalles de la investigación, de acuerdo al nivel de riesgo que obtuve en la pre-evaluación tal y como lo indica la función para niveles de riesgo Medio, Mayor y Alto, procedía a convocar a una

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

reunión con los miembros del Comité de Decisión con el fin de validar el nivel de riesgo identificado y coordinar un plan de mitigación sin afectar la operación del negocio; bajo estas tareas junto con mi equipo de trabajo desarrollé un proceso de comunicación con el equipo central, en el que nuestro líder de proyecto es una de las personas autorizadas junto con mi Subdirector para enviar la convocatoria con el fin de notificar el incidente para coordinar una investigación con el Negocio quien representa al dueño de la información, y de esta forma el Equipo para la Gestión de Incidentes proponía una investigación para identificar claramente con la ayuda del Equipo Central los siguientes puntos:

- El alcance del Incidente.
- Validar la clasificación de la información posiblemente expuesta.
- La cantidad de información involucrada
- ¿Qué partes se ven afectados (por ejemplo, clientes, empleados, etc)
- Cuál es el valor de la Información para su operación (criticidad).
- Todas las acciones que se requieren para mitigar el riesgo.

4.- Proceso de Mitigación de Riesgo.

Este proceso radica en crear un plan de acciones iniciales para los incidentes, proceso que tenía que ser creado por el Equipo para la Gestión de Incidentes, los oficiales de seguridad y el área del negocio a involucrar. Estos procesos eran dirigidos a los incidentes clasificados como riesgos medios, mayores ó altos, de igual forma para algunos incidentes clasificados como Bajos que requerían este proceso que se realizaba mediante una junta para responder al Incidente.

Éstas eran las tareas a validar durante el tiempo de vida del Incidente:

- Confirmar el impacto de la evaluación del riesgo.
- Desarrollar un plan de acción para la solución del Incidente.
- Actualizar el Incidente, reevaluar el impacto y acciones tomadas dentro de un ciclo de mejora continua..
- Determinar los requerimientos adicionales del Incidente (cumplimiento con leyes regulatorias).
- Si se requerían notificaciones durante el Incidente, desarrollar un plan de comunicación.
- Si el usuario requería de notificaciones, desarrollar un plan de comunicación.

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

5.- Funciones en la etapa del manejo del Incidente.

Después del proceso de notificación al Equipo Central y de la coordinación del plan de mitigación, mi responsabilidad como coordinador de la Gestión del Incidente era asegurarme de que todas las acciones a tomar en las etapas previas fueran llevadas a cabo en tiempo y forma, así como informar el proceso del Incidente vía correo electrónico o coordinando juntas en caso de ser necesarias, tener la confirmación por parte de los brazos ejecutores que las acciones estaban siendo realizadas y completadas, así como informar al Equipo Central que las acciones a tomar durante el tiempo de vida del Incidente se estuviesen llevando a cabo para posteriormente realizar una nueva evaluación del impacto y riesgo en caso de ser necesario.

Como puntos primordiales durante la presencia de un Incidente desarrollé los siguientes objetivos a validar:

- Durante todo el tiempo de vida del Incidente, introducir correctamente la información en el software institucional para el seguimiento de los casos y que ésta se encuentre actualizada.
- Notificar al Equipo de Continuidad del Negocio cuando esto proceda.
- Validar que todas las acciones necesarias estén identificadas y ejecutadas de inmediato para contener el Incidente y sus consecuencias.
- Las notificaciones necesarias a las partes afectadas y/o los reguladores.
- Que el Incidente esté cerrado a raíz de la ejecución de todas las acciones necesarias.
- Evaluación y seguimiento del plan de remediación en el proceso de remediación de los Incidentes cuando sea necesario.

6.- Cierre del Incidente.

Una vez que el Equipo para la Gestión de Incidentes tomaba las acciones necesarias para con todas las partes involucradas eran ejecutadas y el riesgo identificado era mitigado, se procedía a identificar las políticas involucradas durante el Incidente para abrir un caso de mejora por cada incidente.

Como miembro de este quipo me encargué de supervisar todas las notificaciones que llegaban a la cuenta de correo electrónico donde brindé mi apoyo al Equipo de Primera Respuesta para realizar los análisis de todas las notificaciones que recibíamos como parte de mis actividades diarias, realizando la evaluación de los Incidentes que se presentaban como parte del nuevo proceso de atención a los incidentes en la seguridad de la información junto con mi equipo de trabajo. También me encargaba de analizar la información obtenida de los eventos/incidentes para construir métricas basadas en la atención de casos con niveles de riesgo, las cuales son reportadas mes con mes a

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

la alta dirección, así como dar cumplimiento a las leyes regulatorias en caso de que se presentara un Incidente que lo ameritara.

3.15 Registro, Seguimiento y Cierre de los casos.

Para documentar todos los casos atendidos se empleaba la Herramienta Institucional para realizar éstas tareas, sin embargo, esta herramienta no contaba con información para medir los tiempos en que cada caso era atendido en toda su ciclo de vida debido a que desde mi punto de vista no se podía hacer un análisis a detalle de la información que nos proporciona esta herramienta para elaborar métricas detalladas y/o poder identificar puntos críticos en los incidentes como lo son:

- Tiempo de escalación del caso.
- Tiempo de respuesta de las administraciones correspondientes.
- Tiempo de vida del caso
- Administración involucrada.
- Asignación del caso.

Debido a esto, elaboré una bitácora de acceso restringido con un usuario y contraseña ubicada en un servidor de archivos al cual el acceso es permitido únicamente a los tres miembros del equipo de atención de incidentes mediante un proceso de aprobación autorizado por el subdirector involucrado, cabe mencionar que se manejan bitácoras distintas por el equipos encargado de los eventos y el equipo encargado de los incidentes.

Es importante mencionar que cada doce meses, he elaborado una nueva bitácora desde Julio del 2010 para evitar consolidar la operación en una única bitácora, misma que contiene los siguientes campos y divisiones:

- Fecha del reporte: este dato lo obtuve de la hora en que recibimos los correos electrónicos en nuestra bandeja de entrada y sirve para medir todo los reportes por cada mes.
- Categoría del reporte: este campo se encuentran las seis categorías a seleccionar de la función con el fin de poder obtener los reportes por cada una de las categorías para analizar la causa raíz en cada categoría.
- Sub categoría del reporte: En cada Categoría que marca la función podemos tener varios escenarios. Por citar un ejemplo, en la pérdida de hardware tenemos Laptops, Teléfonos Celulares, token, etc. Este campo tiene como objetivo realizar una medición en cuanto a los robos de los equipos.

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

- Prioridad del caso: Dependiendo de la importancia del caso podemos tener un Evento con prioridad “Alta y Bajo”, esta prioridad la determina el Equipo para la Gestión de Incidentes en la Seguridad de la Información.
- Clasificación: En este campo podemos tener un Falso Positivo, Evento y un Incidente; se determinó realizando un análisis de riesgos y tiene como objetivo medir la clasificación de los casos recibidos.
- Estatus en General: todos los casos que son registrados deben de ser atendidos hasta lograr cerrar los mismos, en este campo podemos seleccionar “Abierto ó Cerrado”.
- Quién notifica el reporte y a qué Administración pertenece; este dato es importante para validar en caso de ser necesario mayor información del caso.
- Ciudad/País Origen del Evento/Incidente; este dato nos es de gran utilidad para en identificar los estados en donde se puede detectar mayor actividad maliciosa y poder implementar controles compensatorios para mitigar los riesgos.
- Tiempo de Atención (Horas) y Tiempo de vida (días); este dato nos es de gran utilidad para sacar métricas relacionadas al tiempo en que el atendí los reportes y el tiempo en que nuestros brazos ejecutores se tardan en realizar la acción; los campos que contiene esta sección son: Solicitud Recibida, Notificación, Respuesta y Escalación
- Detalles del Caso: En esta sección escribimos a detalle el caso, con el fin de no depender de algún miembro del equipo para conocer el caso.
- Cap. X: Este campo sirve para conocer los casos que aplican esta ley regulatoria.
- Seguimiento: En este campo se detalla todo el seguimiento que se la ha dado a todos los casos con las acciones coordinadas y sus responsables.

Cabe señalar que después del primer año de operación tomé la decisión de segmentar la bitácora de acuerdo a las siete categorías del programa GISI conservando el contenido de los mismos con excepción del campo “Categoría”, con el objetivo de no consolidar toda la información de la operación en un solo control con el fin de evitar que a falta de la disponibilidad de la bitácora no se

CAPÍTULO 3. IMPLEMENTACIÓN DE UN EQUIPO PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

podieran registrar los casos atendidos o verificar el estatus de un Incidente quedando segmentados en las siguientes bitácoras:

- Bitácora para el registro de Phishing.
- Bitácora para el Registro de Malware.
- Bitácora para el Registro de Exposición de Información física y electrónica.
- Bitácora para el Registro de Exposición de datos contenidos en equipos institucionales.
- Bitácora para el Registro del uso inapropiado de la información.
- Bitácora para el Registro de casos relacionados con la Ingeniería Social.

Dentro de cada bitácora elaboré dos secciones distintas, una para el registro de los eventos al cual todos aquellos empleados que tiene acceso a este control pueden ver y otra sección para el registro de Incidentes, la cual requiere de otra contraseña para tener el acceso y fue asignada de forma individual a cada miembro del Equipo para la Atención de Incidentes en la Seguridad de la Información., esta debe cumplir con las especificaciones contenidas dentro del marco normativo en la política de contraseñas institucional.

CAPÍTULO 4

RESULTADOS.

RESULTADOS.

4.1 Incremento en las notificaciones.

Una vez que junto con mi equipo de trabajo terminé de realizar cada una de las tareas que propuse como parte de la implementación de la ahora nueva función GISI, la carga de trabajo se incrementó considerablemente derivado del gran esfuerzo que junto con mis compañeros realicé, la clave de todo esto radicó en, además de tener los contactos y niveles de servicio adecuados, dar a conocer los principales aspectos de la función en cuanto a qué reportar y cómo hacerlo al negocio, es decir a los empleados, ya que de nada hubiese servido el trabajo que realicé si una de nuestras principales alimentaciones en cuanto a notificaciones no tuviera conocimiento de la función.

Una vez que trascurrió el primer año de operación realicé una medición con los datos que obtuve mes con mes con el objetivo de hacer una comparación de nuestros datos, con los datos que la antigua administración registró por mes que en promedio durante un año de actividad fueron cero registros de no eventos, 15 eventos y 2 incidentes durante el periodo en que estuvieron a cargo de la función, estos datos fueron tomados de la bitácora con la que se contaba en su momento, esto para enfatizar que durante el periodo de la antigua administración se dejaron de atender casos que posteriormente resultaron Incidentes que me tocaron atender. Hago la comparación de los datos de mi trabajo con los datos de la antigua administración durante un año debido a que este fue el tiempo dado para medir el progreso del proyecto por parte de la alta dirección, lo anterior con el fin de evaluar y demostrar las actividades realizadas por el nuevo equipo.

- Falta de apego al programa:
 - Analicé el programa con respecto a la capacidad de la institución para la implementación del mismo.
 - Propuse cambios al programa All tomando en cuenta cumplimientos regulatorios aplicables a la institución como IFAI y CAP X
 - Cambié el nombre del programa All a GISI debido a la mala reputación identificada.

- Definición de funciones:
 - Propuse segmentar de la operación en dos equipos distintos.
 - Propuse tener una cobertura de la operación 24 x 7 bajo demanda.

- Elaboré la descripción de puestos y roles para cada equipo.

- Proceso de Atención:
 - Elaboré de un listado de información esencial para una rápida atención de los reportes por cada categoría del programa.
 - Elaboré una bitácora para medir tiempos de atención de todos los casos.
 - Documenté de los cambios realizados.

- Red de contactos:
 - Elaboré una base de datos con el detalle de las funciones de cada administración a involucrar dependiendo del caso.
 - Obtuve acuerdos de trabajo con niveles de servicio por administración.
 - Coordiné pruebas para medir el nivel de servicio.

- Capacitación al negocio:
 - Capacité a personal en todos los niveles de las Institución Financiera.
 - Elaboré una bitácora para medir el registro de empleados capacitados con firma autógrafa
 - Recomendé a negocio nuevos procesos a considerar referentes a seguridad de la información.

- Operación del programa GISI:
 - Brindé calidad en el servicio del programa GISI al tener un promedio de atención no mayor a 15 minutos por reporte recibido.
 - Atendí y orienté al empleado con respecto a qué reportar al equipo GISI.
 - Prioricé casos con base a un nivel de riesgo.

Una fuente indispensable para tener registro de las notificaciones lo fueron las capacitaciones organizadas mes con mes logrando tener un registro mayor a mil empleados durante el primer año de evaluación, aunado a la detección que realizó la administración de Seguridad con la poca infraestructura con la que se contaba en cuanto a los accesos no autorizados a aplicaciones, bases de datos, etc; y otro la gran alimentación en cuanto a notificaciones gracias a la colaboración por parte de los empleados derivado de las llamadas atendidas a para reportar posibles casos.

El resultado que obtuve fue considerablemente mayor con respecto a los datos anteriormente citados ya que en promedio por 12 meses. para los no eventos junto con mi equipo de trabajo

obtuve un incremento del 84%, para los eventos un incremento del 88% y para los incidentes un incremento del 93%, ya que conforme el proyecto avanzaba los empleados capacitados representaron un mayor número de dudas/reportes por lo que los casos a evaluar poco a poco resultaron en que el tiempo no era suficiente para atender todos los casos que recibí, debido a que la carga de trabajo se incrementó en todas las clasificaciones de la función por lo que durante el primer año de operación de la nueva administración de la nueva función obtuve en porcentaje los siguientes resultados como se muestra en la (Figura 4.1)

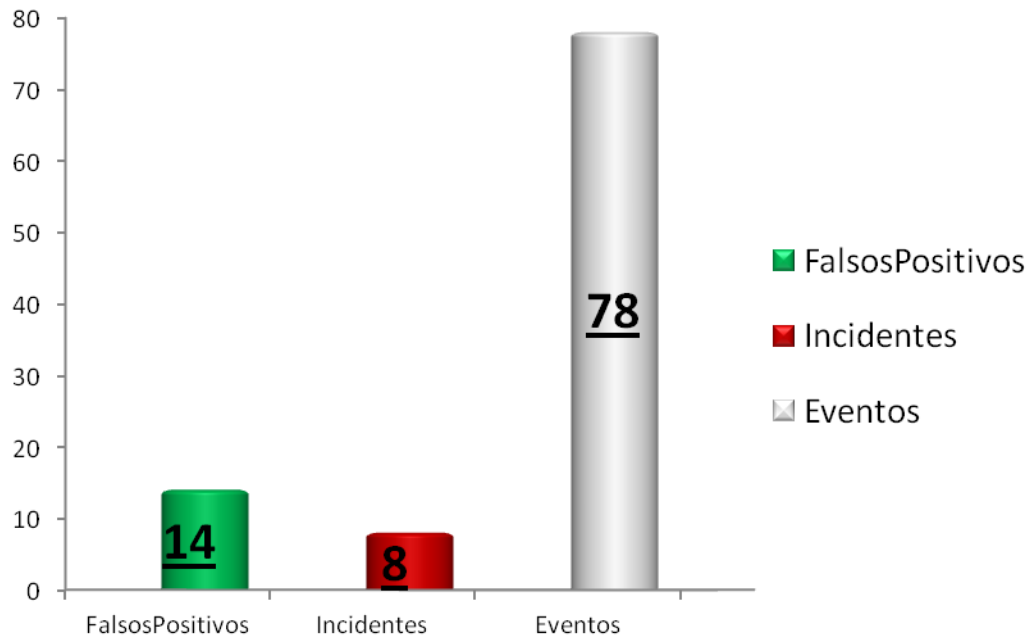


Figura 4.1 Porcentaje de atención por Categoría

Tomando como punto de referencia los datos de la antigua administración mencionados anteriormente, durante el proceso en que junto con mi equipo de trabajo di a conocer la función a los empleados, los no eventos como se muestra en la (figura 4.2) fueron tal vez uno de los puntos en donde más tiempo invertí ya que la mayoría de los empleados al conocer la función siempre tuvieron dudas en cuanto a que debían reportar, curiosamente al principio de nuestra administración atendí dudas con respecto a altas/bajas de usuarios canalizando los reportes con el área indicada sin embargo, conforme la función tuvo mayor presencia las dudas, en cuanto a eventos e incidentes en la seguridad de la Información se incrementaron descartando falsos positivos.

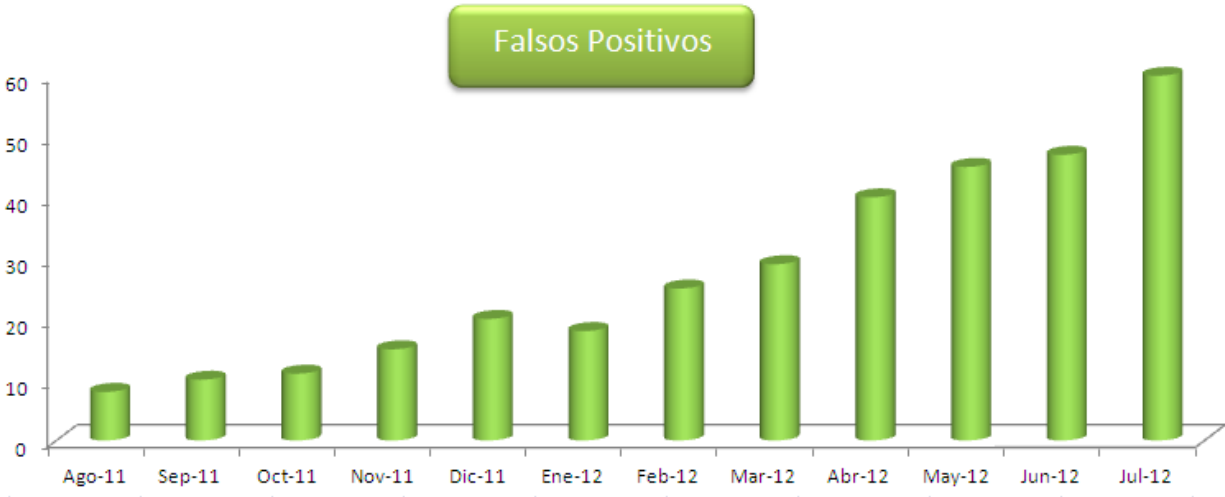


Figura 4.2 Datos no reales de Falsos Positivos atendidos durante el primer año.

Los eventos en la seguridad de la información como se muestra en la (Figura 4.3) fueron el mayor número de reportes que atendí y registré en nuestro control y herramienta Institucional, eventos como spam, phishing, evaluaciones con respecto al robo de lap-tops y equipos de telefonía celular e infecciones vía código malicioso (spyware, adware) sin llegar a comprometer la información de los equipos.

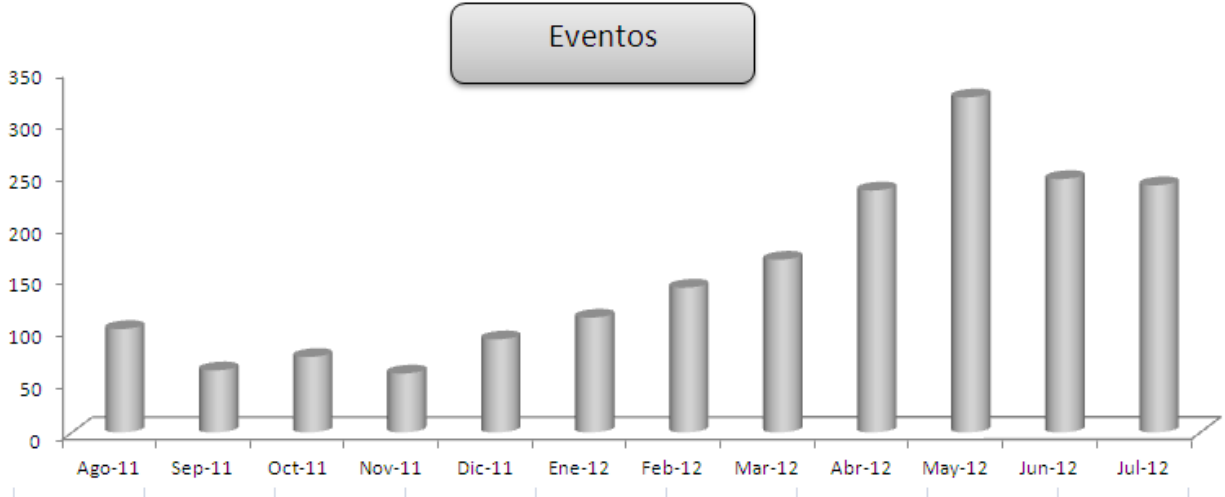


Figura 4.3 Datos no reales de eventos atendidos durante el primer año

Mantener el número de incidentes razonablemente bajo es muy importante para proteger los procesos de negocio en la Institución Financiera por ello uno de los objetivos que siempre busqué cuando comencé con este proyecto fue dejar a un lado el concepto “Seguridad por Oscuridad” ya

que el hecho de no registrar incidentes no significa que no existan, significa que simplemente puede que sucedan y no se detecten, suceso común en varias Instituciones hoy en día como lo fue en su momento con la antigua administración de la función. Conforme avanzó el proyecto como se aprecia en la (Figura 4.4) tuve más notificaciones de brechas en la Seguridad de la Información, ya que al momento en que realicé la evaluación de los casos más y más detalles salían a flote como puntos a mejorar lo cual me obligó a tener una mayor visión, comunicación y conocimiento de las Administraciones dentro de la Dirección donde laboro, para en caso de necesitar la rápida ejecución de alguna acción de mitigación esta fuera atendida por alguno de mis compañeros como prioridad, esto con todos los empleados dentro de la Dirección de Seguridad tuve una mejor comunicación en cuanto a trabajo en equipo enfocado a la protección de los activos informáticos.

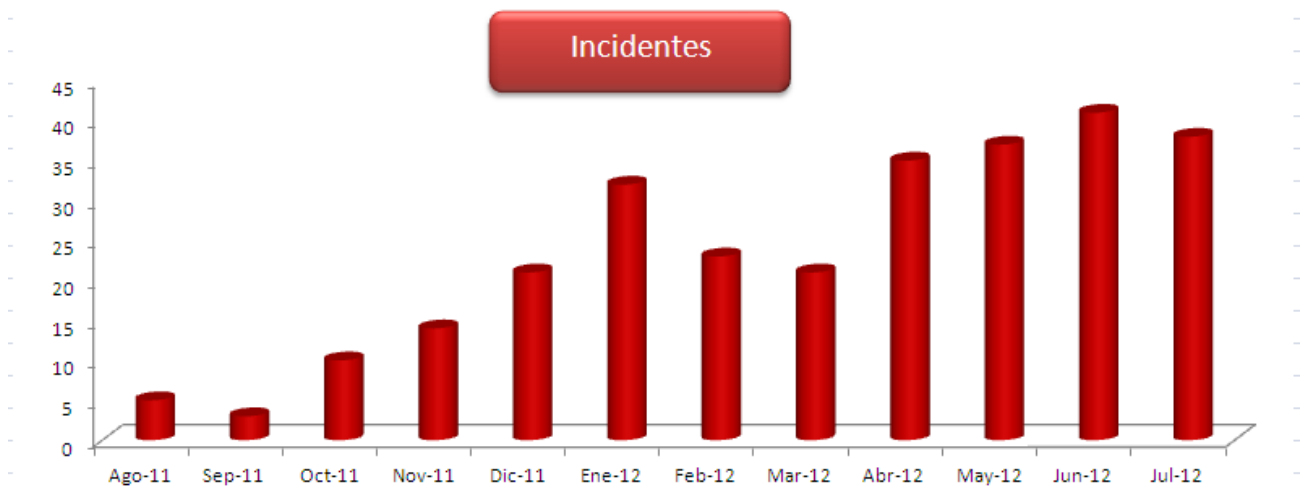


Figura 4.4 Datos no reales de incidentes en la seguridad de la información atendidos durante el primer año.

Mes con mes continué conociendo aplicaciones y áreas de la Institución Financiera derivado de las notificaciones que recibí de los empleados en donde existían oportunidades de mejora para proteger sus procesos desde el punto de vista Seguridad de la Información por lo que la carga de trabajo en cuanto a la detección de afectaciones en la Seguridad de la información se fue incrementando considerablemente con respecto a los datos de la antigua administración por lo que en varias ocasiones tuve que darle prioridad a aquellos casos en donde el nivel de riesgo que en su momento evalué, representó un mayor impacto tanto financiero, como al prestigio y un cumplimiento con alguna ley regulatoria para la institución financiera, cuidando siempre los tiempos de vida de éstos casos ya que entre más tiempo tardaban en ejecutarse las acciones de mitigación la brecha continuaba latente y con esto el posible compromiso de la información.

4.2 Métricas.

Con el fin de tener un control del progreso de las actividades que llevé a cabo dentro de este proyecto, las métricas que determiné realizar fueron un factor de suma importancia que me ayudaron a mostrar el valor que aporté a la Institución Financiera con la correcta implementación y operación de la función que junto con mi equipo de trabajo realicé, teniendo en mente el objetivo de siempre buscar una mejora continua dentro de nuestra Gestión para las brechas en la Seguridad de la Información transformando el lenguaje técnico en reducción de riesgos y costos para la Institución.

Para la selección de métricas primero tomé en cuenta aquellas que indica la función como lo son la medición de los no eventos, eventos e incidentes en la seguridad de la Información con un total de 3320 casos atendidos durante el año de la implementación en cada una de las siete categorías que marca la función como se aprecia en la (Figura 4.5) con el objetivo de cumplir con todos los puntos que establece la misma.

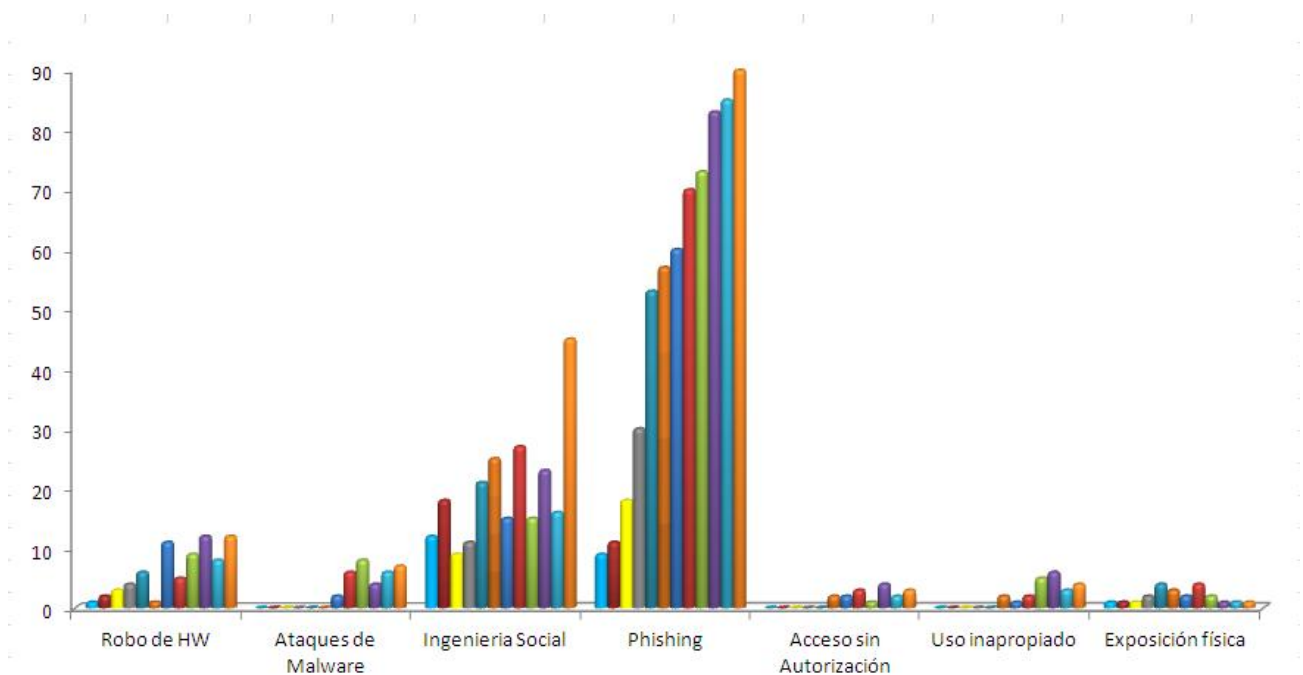


Figura 4.5 Datos no reales relacionados a la Distribución de casos atendidos por Categoría durante el primer año.

Adicional a las métricas citadas anteriormente, junto con mi equipo de trabajo determiné tomar en cuenta otros aspectos a medir para mostrar la importancia de nuestro trabajo tomando en cuenta como prioridad el cumplimiento con leyes regulatorias y la reducción de riesgos identificados:

- Número de incidentes por nivel de riesgo
- Número de incidentes por Administración.
- Número de incidentes relacionados con terceros.
- Número de incidentes derivados de falta/debilidades en nuestros controles.
- Número de Eventos/Incidentes que aplican cumplimiento Regulatorio.
- Tiempo de Atención del IMT (Calidad de Servicio).
- Tiempo de Escalación del IMT.
- Tiempo de vida (Seguimiento).
- Número de riesgos identificados y mitigados.

Para la selección de las actividades a medir dentro del Equipo para la Gestión de Incidentes en la Seguridad de la Información tuve al principio varias dudas ya que mi función principal fue operar una función no enfocada a la producción monetaria, derivado de lo anterior, fue difícil establecer parámetros de medición que dieran valor a nuestro trabajo con respecto a reducción de costos para la Alta Dirección, por ello tomé en cuenta puntos estratégicos con el objetivo de medir la aplicación de los controles existentes para proteger la información en cada una de las administraciones del banco y dar una retroalimentación de este dato al negocio, con esto pude tener datos para mostrar los parámetros del cumplimiento por parte de todos los empleados en cuanto a la aplicación de los controles existentes para el manejo seguro de la información como por ejemplo el cifrado de correos electrónicos, el cumplimiento para con la clasificación de la información que se maneja dentro de la Institución y ejercicios de escritorios limpios los cuales radican en no dejar a la vista información de la Institución sobre los escritorios de trabajo.

Durante el primer año de actividad que fue la parte más difícil y compleja en general, me di cuenta que lo único que había logrado es dar el primer paso hacia un nuevo objetivo planteado por nosotros mismos ya que apenas comencé a poder observar algunos incidentes en la Seguridad de la Información y algunos empleados comenzaban a tomar en cuenta el tema Seguridad de la Información para la elaboración de sus procesos, aprobaciones de documentos y clasificación de la información por lo que el paso que tomé fue la base para que hoy en día exista una función encargada del monitoreo de la red y los accesos a servidores que básicamente es una fuente de notificaciones para nuestra función, por lo que hoy en día derivado del trabajo que realicé junto con mi equipo de trabajo la alta dirección propuso la fusión de las dos Funciones (Monitoreo y GIS) para que se convirtiera en una Administración dentro de la Dirección de Riesgos en la Seguridad de la Información.

CONCLUSIONES

CONCLUSIONES

Este proyecto que junto con mi equipo de trabajo coordiné y desarrollé, tuvo muy buenos resultados dentro la Dirección de la Seguridad Informática, cumpliendo con el objetivo del proyecto de lograr la implementación del equipo para la gestión de incidentes en la seguridad de la información en un año para que posteriormente este proyecto se diera a conocer a nivel institucional en todas las sedes del país, ya que junto con mi líder de proyecto encontré la forma de adaptar nuevos procesos relacionados con la Seguridad de la información ante el negocio para darle valor al trabajo que realicé, colaborando con el objetivo y estrategia de la Institución al lograr minimizar los riesgos identificados a niveles marcados institucionalmente como aceptables y en específico con el desarrollo de la Dirección de la Seguridad Informática; con esto, la función GISI comenzó a tener una importante presencia en todas las Direcciones de la Institución Financiera, lo cual incrementó las notificaciones y la carga de trabajo conforme avanzó el desarrollo del proyecto logrando que los empleados capacitados pudiesen dudar antes de cometer una violación a las políticas de seguridad de la información así como nuevos retos dentro del mismo.

Como parte de la implementación de la función ahora nombrada GISI, uno de los puntos que logré exitosamente cumplir consistió en que los empleados conocieran lo que significa la función GISI su objetivo y los alcances de la misma, para que en caso de tener una duda, con respecto a los casos que gestionó, conocieran el canal para reportar algún evento/incidente que afectará la Seguridad de la Información en la Institución. De igual forma, estando esta función enfocada al servicio de la Institución, la interacción que tuve con los empleados al resolver sus dudas me ayudo a conocer un poco más el negocio y saber qué es lo que se está protegiendo para darle la debida prioridad a cada situación que derivara en un posible impacto financiero, a la marca y un posible cumplimiento regulatorio.

En ese contexto, debido a la capacitación que impartí mes con mes, logré que los empleados en cada Administración tuvieran comunicación con el Equipo para la Gestión de Incidentes en la Seguridad de la Información, para que de esta forma, se lograra enganchar a los empleados de las diferentes Administraciones e incrementar los posibles casos a reportar día a día; así mismo, evalué diferentes situaciones en donde realicé análisis de riesgos usando la metodología institucional para casos en cada una de las seis categorías que marca la función; con esto, logré

identificar y realizar procedimientos para optimizar la operación, ya que con una mayor presencia de la función GISI dentro de la Institución Financiera, surgió la necesidad de contratar más recursos para atender la carga de trabajo la cual se incrementó un 200% tomando como referencia los registros de los últimos seis meses de la antigua Administración encargada de la operación del Programa, esto en comparativa con los primeros tres meses de nuestra operación. Sin dudarlo, el trabajo que realicé con respecto a los acuerdo de servicio, el inventario de contactos, la actualización de los procedimientos, la capacitación y las tareas especificadas dentro del capítulo tres, lograron que hoy en día la institución financiera se encuentre preparada para poder identificar posibles incidentes y una vez confirmados poder tener una rápida gestión de los mismos.

Por último, es necesario subrayar que las Instituciones Financieras en nuestro país pertenecen al grupo de las primeras empresas que deben tomar en cuenta la implementación de la Seguridad Informática dentro de su negocio, tal y como algunas ya lo han empezado a realizar, lo anterior con el fin de que progresivamente todas las Instituciones Financieras y otras empresas se incorporen a este gran tema que aparentemente es joven para el ambiente laboral y que poco a poco ha dado de que hablar derivado de las fugas de información que sufren las Instituciones Financieras particularmente en todo el mundo.

APÈNDICE

"Capítulo X

Del uso del servicio de Banca Electrónica

Sección Cuarta

De la seguridad, confidencialidad e integridad de la información transmitida, almacenada o procesada a través de Medios Electrónicos

Artículo 316 Bis 10.- Las Instituciones que utilicen Medios Electrónicos para la celebración de operaciones y prestación de servicios, deberán implementar medidas o mecanismos de seguridad en la transmisión, almacenamiento y procesamiento de la información a través de dichos Medios Electrónicos, a fin de evitar que sea conocida por terceros. Para tales efectos, las Instituciones deberán cumplir con lo siguiente:

- I. Cifrar los mensajes o utilizar medios de comunicación Cifrada, en la transmisión de la Información Sensible del Usuario procesada a través de Medios Electrónicos, desde el Dispositivo de Acceso hasta la recepción para su ejecución por parte de las Instituciones, a fin de proteger la información a que se refiere el Artículo 117 de la Ley, incluyendo la relativa a la identificación y Autenticación de Usuarios tales como Contraseñas, Números de Identificación Personal (NIP), cualquier otro Factor de Autenticación, así como la información de las respuestas a las preguntas secretas a que se refiere el penúltimo párrafo del Artículo 316 Bis 3 de estas disposiciones.

Para efectos de lo anterior, las Instituciones deberán utilizar tecnologías que manejen Cifrado y que requieran el uso de llaves criptográficas para asegurar que terceros no puedan conocer los datos transmitidos.

Las Instituciones serán responsables de la administración de las llaves criptográficas, así como de cualquier otro componente utilizado para el Cifrado, considerando procedimientos que aseguren su integridad y confidencialidad, protegiendo la información de Autenticación de sus Usuarios.

Tratándose de Pago Móvil, Banca Telefónica Voz a Voz y Banca Telefónica Audio Respuesta, podrán implementar controles compensatorios al Cifrado en la transmisión de información a fin de protegerla.

- II. Las Instituciones deberán Cifrar o truncar la información de las cuentas u operaciones de sus Usuarios y Cifrar las Contraseñas, Números de Identificación Personal (NIP), respuestas secretas, o cualquier otro Factor de Autenticación, en caso de que se almacene en cualquier componente de los Medios Electrónicos.
- III. En ningún caso, las Instituciones podrán transmitir las Contraseñas y Números de Identificación Personal (NIP), a través de correo electrónico, servicios de mensajería instantánea, Mensajes de Texto SMS o cualquier otra tecnología, que no cuente con mecanismos de Cifrado.

Se exceptúa de lo previsto en esta fracción a las Contraseñas y Números de Identificación Personal (NIP) utilizados para acceder al servicio de Pago Móvil, siempre y cuando las Instituciones mantengan controles para que no se pongan en riesgo los recursos y la información de sus Usuarios. Las Instituciones que pretendan utilizar los controles a que se refiere el presente párrafo deberán obtener la previa autorización de la Comisión, para tales efectos.

Asimismo, la información de los Factores de Autenticación Categoría 2 a que se refiere el Artículo 310 de las presentes disposiciones, utilizados para acceder a la información de los estados de cuenta, podrá ser comunicada al Usuario mediante dispositivos de audio respuesta automática, así como por correo, siempre y cuando esta sea enviada utilizando mecanismos de seguridad, previa solicitud del Usuario y se hayan llevado a cabo los procesos de Autenticación correspondientes.

- IV. Las Instituciones deberán asegurarse de que las llaves criptográficas y el proceso de Cifrado y descifrado se encuentren instalados en dispositivos de alta seguridad, tales como los denominados HSM (Hardware Security Module), los cuales deberán contar con prácticas de administración que eviten el acceso no autorizado y la divulgación de la información que contienen.

Artículo 316 Bis 12.- En caso de que la Información Sensible del Usuario sea extraída, extraviada o las Instituciones supongan o sospechen de algún incidente que involucre accesos no autorizados a dicha información, deberán:

- I. Enviar por escrito a la Dirección General de la Comisión encargada de su supervisión, dentro de los cinco días naturales siguientes al evento de que se trate, la información que se contiene en el Anexo 64 de las presentes disposiciones.
- II. Llevar a cabo una investigación inmediata para determinar si la información ha sido o puede ser mal utilizada, y en este caso deberán notificar esta situación, en los siguientes 3 días hábiles, a sus Usuarios afectados a fin de prevenirlos de los riesgos derivados del mal uso de la información que haya sido extraída, extraviada o comprometida, debiendo informarle las medidas que deberán tomar. Asimismo, deberán enviar a la Dirección General de la Comisión encargada de su supervisión, el resultado de dicha investigación en un plazo no mayor a cinco días naturales posteriores a su conclusión.

GLOSARIO DE TÉRMINOS

- Adware..... Código que tiene por objetivo mostrar publicidad mientras se navega por Internet.
- Accesos No Autorizados: Cuando una persona logra obtener el acceso lógico o físico sin la autorización de la red, el sistema, la aplicación, a la información que resguarda.
- Activos Informáticos..... Elementos tangibles e intangibles que tiene valor para la organización.
- Amenazas.....Una causa potencial de un incidente indeseado, el cual puede resultar en un daño a un sistema u organización.
- Análisis de Riesgos.....Proceso de Identificación y Estimación del riesgo.
- Antivirus..... Base de datos cuya función es detectar y eliminar virus informáticos y otros programas peligrosos llamados malware
- Ataques de día cero..... Ataque realizado mediante un código malicioso con el fin de explotar vulnerabilidades, de algún programa o programas antes de que se conozcan las mismas
- Autenticación de la Información..Garantizar que los participantes en una comunicación sean quien dicen ser, es decir, proceso de identificación de una parte ante las demás, de una manera fehaciente.
- BCP.....Plan para la Continuidad del Negocio
- Biometría.....Tecnología basada en el reconocimiento o identificación de una característica física e intransferible de las personas, como por ejemplo la huella digital.
- Bitácora.....Formato utilizado para llevar un registro de actividades
- Brechas en la seguridad de la Información..... Factor Interno/Externo que tiene el potencial de causar un extensivo daño a una Institución, clientes entidades relacionadas.

- Confidencialidad de la Información.....Garantizar que la Información solo pueda ser accedida por las partes autorizadas; por nadie más.
- Criticidad de la Información.....Impacto que posee en cuanto a la afectación de la operación.
- Diagrama de Flujo.....Representación gráfica de un Algoritmo.
- Estafas Nigerianas..... Tienen el propósito de ganar la confianza de la víctima para involucrarla en un supuesto negocio y/o transacción (fraude) con el fin de obtener una ganancia económica.
- Evento.....Representan un riesgo menor o insignificante
- Gestión.....Proporciona la fundamentación y la justificación para casi todas las actividades relacionadas con la S.I.
- Impacto..... Cambio adverso al nivel de los objetivos del negocio alcanzados
- Incidente..... Representan un riesgo masivo, mayor o moderado
- Información sensible.....Información personal privada de un individuo
- Infraestructura Tecnológica.....Base primordial de cualquier empresa y permite la optimización de sus recursos, el aumento del valor de su empresa y una respuesta más rápida a los requerimientos del mercado.
- Ingeniería de Instalación.....Diagrama de instalación de una tecnología.
- Ingeniería Social.....El uso del engaño, la manipulación o la persuasión para obtener información mediante diferentes medios, algunos no técnicos dirigidos a los empleados, en general por medio de un correo electrónico, una llamada telefónica o en persona.
- Integridad de la Información.... Protege activos del sistema contra modificaciones, alteraciones, borrado, inserción sin la previa autorización y justificación
- Internet..... Interconexión de redes de datos que permite a las computadoras conectadas comunicarse directamente entre sí.
- Lista Blanca.....Registros de datos que derivado de un análisis cuentan un privilegio en particular.

Malware.....	Código malicioso diseñado para dañar o hacer o realizar acciones no autorizadas en un sistema informático.
Mecanismos de Control de Acceso.....	Control en un sistema especializado en detectar los intentos de acceso, permitiendo el paso de las entidades autorizadas, y denegando el paso a todas las demás. Involucra medios técnicos y procedimientos operativos.
Negación de servicio... ..	Ataque a un Sistema/Aplicación web que causa que un servicio o recurso sea inaccesible a los usuarios legítimos
No evento.....	Cualquier caso en donde no existe un compromiso de información manejada, almacenada y distribuida por la Institución.
Nodo B.....	Equipo de telecomunicación para una red UMTS.
OLA´s & SLA´s.....	Nivel de Acuerdo Operacional y Nivel de Acuerdo de Servicio.
Página Web.....	Documento creado en formato HTML que es parte de un grupo de documentos hipertexto o recursos disponibles en Internet
Perímetro Físico.....	Frontera física que define un dominio de seguridad o zona en la que se aplica una determinada política de seguridad o se ha implantado una determinada arquitectura de seguridad.
Phishing.....	Intento de obtener información confidencial de los clientes mediante el engaño o la manipulación utilizando medios electrónicos, principalmente el correo electrónico
Política de Seguridad.....	Descripción bajo la forma de reglas, en la que se incluyan las propiedades de Confidencialidad, Integridad y Disponibilidad de la información en la medida requerida por una Organización
Rack.....	Soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones
Red Inalámbrica.....	Permite establecer vínculos entre computadoras y otros equipos informáticos sin necesidad de instalar un cableado

Redes de Datos.....	Conjunto de dispositivos conectados entre sí mediante uno o más medios de transmisión a fin de llevar a cabo la transferencia eficiente y confiable de información
Riesgo.....	Probabilidad de ocurrencia de un evento o transacción que causa pérdida financiera o daño a la organización, a su personal, a sus activos o a su imagen
Riesgo Inherente.....	Riesgo percé de la información, es decir, es un riesgo que no se puede mitigar, es inherente a la información.
Riesgo Residual.....	Es el riesgo resultante derivado de un tratamiento a un riesgo, es decir, el riesgo no siempre puede ser mitigado.
Script.....	Conjunto de instrucciones generalmente almacenadas en un archivo de texto que deben ser interpretados línea a línea en tiempo real para su ejecución
Seguridad de la Información....	Tiene por objetivo la protección de la Integridad, Confidencialidad y Autenticidad de la información, así como un manejo seguro desde la creación, almacenamiento y destrucción de la misma.
Seguridad Informática.....	Tiene como función proteger la infraestructura Tecnológica y los datos contenidos en esta.
Seguridad Perimetral.....	Integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de intrusos en instalaciones especialmente sensibles.
Spam.....	Correo no deseado
Spyware.....	Código Malicioso que recopila información de una PC para transmitirla a una entidad externa sin una autorización
Token.....	Dispositivo electrónico usado para la autenticación en un servicio computarizado
Topología de Red.....	Descripción de la forma en la que está diseñada la red, físicamente o lógicamente en donde dos o más dispositivos se conectan a un enlace(s)
UMTS.....	Sistema universal de telecomunicaciones móviles.

- URL.....Cadena de caracteres con la cual se asigna una dirección única a cada uno de los recursos de información disponibles en la Internet
- Vulnerabilidades..... Una debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas

REREFENCIAS

1. Computer Security Incident Handling Guide Special Publication 800-61. Recommendations of the National Institute of Standards and Technology, U.S. Department of Commerce.
2. Information Security, Guide for Conducting Risk Assessment 800-30, National Institute of Standards and Technology, U.S Department of Commerce.
3. Risk Analysis and treatment guide, Clusif Mehari.
4. ISO 7498-2 Arquitectura de Seguridad.