



UNIVERSIDAD LA SALLE

FACULTAD DE NEGOCIOS

Con Reconocimiento de Validez Oficial de Estudios de la Secretaría de Educación
Pública según acuerdo número No 954315 De fecha 30 de Octubre de 1995.

ELABORACIÓN DE UN ESTUDIO DE CASO

**“Propuesta de protocolos para atención de incidentes de
seguridad de la información en el sector bancario mexicano:
banco C”**

**QUE PARA OBTENER EL GRADO DE
MAESTRO EN TECNOLOGÍAS DE LA INFORMACIÓN EN LA
DIRECCIÓN DE NEGOCIOS.**

**PRESENTA:
Alain Silvers Salas Vázquez.**

Asesor de Tesis: Mtro. Marco Antonio Siller Jiménez.

Ciudad de México, 2024.

Ciudad de México, a 6 de febrero de 2024.

MTRO. GABRIEL NUÑEZ GONZÁLEZ
DIRECTOR DE GESTIÓN ESCOLAR
UNIVERSIDAD LA SALLE
P R E S E N T E

Le informo que el (la) C.

Alain Silvers Salas Vázquez

Egresada (o) de la Facultad de: Negocios

de la **UNIVERSIDAD LA SALLE**, de la Maestría en: _____

TECNOLOGÍAS DE INFORMACIÓN EN LA DIRECCIÓN DE NEGOCIOS

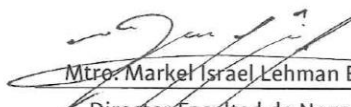
Con reconocimiento de validez oficial de estudios de la Secretaría de Educación

Pública según acuerdo número 974226 de fecha 25 de julio de 1997

Ha elaborado el trabajo de estudio de caso titulado: "Propuesta de protocolos para atención de incidentes de seguridad de la información en el sector bancario mexicano: banco "C"."

De conformidad con la modalidad para la obtención de grado aprobada para esta Maestría de acuerdo a lo establecido en el Reglamento General de las Universidades La Salle Integrantes del Sistema Educativo de las Universidades la Salle.

Cumplió con todos los requisitos y el trabajo que fue elaborado bajo la conducción del Mtro. Marco Antonio Siller Jiménez que fungió como asesor, tiene la calidad suficiente para ser la base de sustentación de su Examen de Grado por lo que se le autoriza presentarlo.



Mtro. Markel Israel Lehman Elizondo
Director Facultad de Negocios

DEDICATORÍA

Le dedico el resultado de este trabajo a toda mi familia. Principalmente, a mis padres, Eva y Silverio, quienes son el faro de luz que ilumina mi camino en la oscuridad, que por su amor incondicional y por su ejemplo de constancia y trabajo he podido superar los obstáculos de la vida. Todo lo bueno que soy es por ustedes, así mismo, todos los logros que he realizado y voy a realizar son por y para ustedes.

Red Light, 2017.

ÍNDICE

Glosario.....	8
Prefacio.....	10
1. Introducción	11
2. Objetivo	13
3. Antecedentes	14
4. Situación Actual.....	21
5. Problemática	22
6. Desarrollo.....	23
6.1 Desarrollo de modelo de gestión de incidentes.....	23
6.1.1 Fase 1: Diseño de la Gestión de Incidente.	23
6.1.1.1 Objetivo.....	23
6.1.1.2 Políticas.	23
6.1.1.3 Definición de los roles y actividades del equipo de Trabajo.	23
6.1.2 Fase 2: Proceso de la Gestión del Incidente.....	24
6.1.2.1 Reportar Incidente.	25
6.1.2.2 Registrar el Incidente.	26
6.1.2.3 Categorizar el Incidente.	27
6.1.2.4 Priorización del Incidente.....	29
6.1.2.5 Investigación y Diagnóstico del Incidente.	31
6.1.2.6 Solución y Documentación del Incidente.....	32
6.1.3 Fase 3: Actividades Post Incidentes.....	33
6.1.3.1 Lecciones aprendidas.	33
6.1.3.2 Uso de evidencias recolectadas.	33
6.1.4 Fase 4: Tratamiento para los incidentes recurrentes.....	34
6.1.4.1 Soluciones basadas en las categorías de los incidentes.....	34
6.2 Herramientas de Soporte	34
6.2.1 ServiceNow.....	34
6.2.2 Freshservice.....	35
6.2.3 Mesa de servicio de JIRA	36
6.2.4 OpsGenie	36

6.2.5 LiveAgent	37
7. Resultados	38
7.1 Flujo de trabajo.	38
7.2 Objetivo: Crear una base de datos precisa con la información generada de los incidentes reportados.	38
7.2.1 Plan.	38
7.2.2 Ejecución.	39
7.2.3 Resultados.	39
7.2.4 Plan de Mejora.	40
7.3 Objetivo: Identificar los tipos de subcategoría y niveles de priorización para la atención de los incidentes.	41
7.3.1 Plan.	41
7.3.2 Ejecución.	41
7.3.3 Resultados.	44
7.3.4 Plan de Mejora.	47
7.4 Objetivo: Establecer una solución por cada subcategoría de los incidentes recurrentes.	49
7.4.1 Plan.	49
7.4.2 Ejecución	49
7.4.3 Resultados.	51
7.4.4 Plan de Mejora.	53
8. ANALISIS DE RESULTADOS.	57
9. CONCLUSIONES	58
9. Referencias	59

ÍNDICE DE GRÁFICAS, TABLAS E IMÁGENES.

Gráfica 1. Área única responsable de la seguridad digital en la entidad / institución financiera	14
Gráfica 2. Marcos de seguridad y/o estándares internacionales adoptados.....	15
Gráfica 3. Procesos / programas respecto a la seguridad digital implementados actualmente por las entidades e instituciones financieras.....	15
Gráfica 4. Eventos (ataques exitosos y ataques no exitosos) de seguridad de la información contra las entidades e instituciones financieras que se han identificado durante los últimos doce meses	16
Gráfica 5 Frecuencia en la ocurrencia de eventos de seguridad de la información contra las entidades e instituciones financieras	17
Gráfica 6 Estrategias de Priorización frente a incidentes de seguridad digital	17
Gráfica 7 Estrategias de Contención frente a incidentes de seguridad digital	18
Gráfica 8 Estrategias de Respuesta frente a incidentes de seguridad digital	18
Gráfica 9 Estrategias de Recuperación frente a incidentes de seguridad digital	18
Gráfica 10 ¿La institución financiera ofrece un mecanismo para que sus de servicios financieros reporten incidentes de seguridad de la información (incluyendo ciberseguridad y fraudes ocurridos a través de medios digitales)?	19
Gráfica 11 ¿La institución financiera a la cual usted pertenece cuenta con un plan de comunicaciones que permita informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida?	19
Gráfica 12 ¿Conoce algún mecanismo para reportar incidentes de seguridad de la información sufridos por la institución financiera a la cual usted pertenece ante una autoridad de regulación en México?	20
Gráfica 13 ¿La institución financiera a la cual usted pertenece reporta los incidentes de seguridad de la información sufridos ante una autoridad de procuración de justicia en México?	20
Gráfica 14. Porcentaje de Incidentes por categoría en el primer año.	40
Gráfica 15. Porcentaje de Incidentes por categoría al segundo año.	41
Gráfica 16. Subcategorías de Facebook.....	45
Gráfica 17. Subcategorías de Twitter.....	45
Gráfica 18. Subcategorías de Clear Web.....	46
Gráfica 19. Porcentaje de los incidentes a los primeros años por subcategoría.....	46
Gráfica 20. Porcentaje por prioridad de los incidentes.	47
Gráfica 21. Nuevo porcentaje por prioridad de los incidentes.	48
Gráfica 22. Porcentaje de incidentes por niveles de atención.	51
Gráfica 23. Porcentaje de atención de 1er nivel por áreas.....	52
Gráfica 24. Porcentaje de atención de 2° nivel por áreas.	52
Gráfica 25. Porcentaje de incidentes atendidos por área.....	53
Gráfica 26. Promedio de horas para la atención de incidentes por categoría.	54
Gráfica 27. Promedio de horas para la atención de incidentes por categoría después del modelo.	
Gráfica 28. Comparación del promedio de horas para la atención de incidentes por categoría antes y después del modelo de gestión de incidentes	55

ÍNDICE DE TABLAS.

Tabla 1. <i>Categorías de Impacto de Incidentes.</i>	29
Tabla 2. <i>Categorías de Urgencia de Incidentes.</i>	29
Tabla 3. <i>Determinación del nivel de prioridad.</i>	30
Tabla 4. <i>Campos relacionados a la apertura de incidentes.</i>	39
Tabla 5. <i>Número de Incidentes por categoría en el primer año.</i>	39
Tabla 6. <i>Número de Incidentes por categoría al segundo año.</i>	40
Tabla 7. <i>Número de Incidentes por subcategoría al segundo año.</i>	42
Tabla 8. <i>Impacto de Incidentes por subcategoría.</i>	42
Tabla 9. <i>Urgencia de Incidentes por subcategoría.</i>	43
Tabla 10. <i>Prioridad de atención por subcategoría.</i>	43
Tabla 11. <i>Asociación de Categorías con subcategoría.</i>	44
Tabla 12. <i>Nueva valorización de Urgencia de Incidentes por subcategoría.</i>	47
Tabla 13. <i>Nueva Prioridad de atención por subcategoría.</i>	48
Tabla 14. <i>Atención de incidentes por subcategoría.</i>	49
Tabla 15. <i>Niveles de incidentes por subcategoría.</i>	51

ÍNDICE DE IMÁGENES.

Imagen 1. <i>Actividades del Gestor de Incidentes.</i>	32
Imagen 2. <i>Actividades para la Gestión del Incidente.</i>	56

Glosario.

AMENAZA: una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización.

COBIT: El marco principal de COBIT guía a las organizaciones a través de las mejores prácticas y la estandarización de los procesos de TI y la infraestructura. El objetivo es alinear la TI con los objetivos comerciales generales al poner a TI en la misma página que el resto de la empresa.

CONFIDENCIALIDAD: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

DISPONIBILIDAD: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

EVENTO: aparición o cambio de un conjunto particular de circunstancias.

EVENTOS EN SEGURIDAD DE LA INFORMACIÓN: ocurrencia identificada de un sistema, servicio o estado de la red que indica una posible violación de la política de seguridad de la información o el fracaso de los controles, o una situación previamente desconocida que puede ser pertinente a seguridad.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: procesos para detectar, informar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

GESTIÓN: acción y efecto de administrar.

INCIDENTE EN SEGURIDAD DE LA INFORMACIÓN: un evento o una serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de la organización y amenaza la seguridad de la información.

INFORMACIÓN: es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada.

INTEGRIDAD: propiedad de la información relativa a su exactitud y completitud.

ITIL: ITIL es un marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de información.

RIESGO: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

RIESGO DE SEGURIDAD DE LA INFORMACIÓN: potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

SEGURIDAD DE LA INFORMACIÓN: preservación de la confidencialidad, la integridad y la disponibilidad de la información.

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN - SGSI: sistema de gestión diseñado para asegurar controles de seguridad suficiente y proporcional que protejan los activos de información y brinden confianza a las partes interesadas.

Prefacio.

El contenido de la propuesta del presente documento, tiene como objetivo dar respuesta a mis propias necesidades laborales para buscar, adaptar y documentar un procedimiento adecuado de atención al proyecto denominado “Incidentes de Seguridad de la Información”, el cual, no había generado el interés necesario por la institución financiera, si no hasta que la regulación empezó a generar revisiones, a aplicar multas y sanciones a las instituciones que no las atendían, lo que generó que se estableciera como prioridad de atención por parte del banco.

Al mismo tiempo, estaba cursando materias de la Maestría en las que se mencionaban las normas y mejores prácticas de atención de Incidentes, las cuales, consideré como guías rectoras para adaptar a mi trabajo en la institución y que son el fundamento del desarrollo teórico de este documento, el cual se estructura en 9 capítulos, los cuales se resumen a continuación:

- En el primero se describió el contexto, la misión y visión de la institución.
- El segundo capítulo se detallan los objetivos que se buscan cumplir a través de la investigación.
- El tercer capítulo se describen los antecedentes donde se muestra en qué momento se encuentra la institución.
- En el cuarto capítulo se habla de la situación actual que vive la institución.
- En el quinto capítulo se describió la problemática que enfrenta la empresa.
- En el capítulo sexto se documenta el desarrollo del modelo de gestión de incidentes de seguridad.
- En el capítulo séptimo se analizan los resultados obtenidos por cada objetivo obtenido de la implementación del modelo de gestión de incidentes.
- Y finalmente en el capítulo octavo y noveno culminan la investigación con el análisis de los resultados, las conclusiones y recomendaciones encontradas durante todo el proceso, anexando toda la información necesaria para la investigación.

1. Introducción.

La organización objeto de este estudio y que, por razones de confidencialidad se omite su nombre y se le asigna un nombre genérico: Banco C, es una institución de banca que surge con más de cuarenta años de experiencia en un negocio de financiamiento de venta de muebles y ropa en tiendas, con el objetivo de atender a sus clientes mediante una oferta integral de servicios bancarios.

La Secretaría de Hacienda y Crédito Público (SHCP) le otorgó el 21 de noviembre de 2006 el registro de autorización para operar como institución de Banca Múltiple, pero fue hasta el 21 de mayo de 2007 cuando iniciaron operaciones, y que con más de 14 años Banco C busca ofrecer a la población de bajos ingresos los servicios bancarios que les permitan administrar mejor sus recursos a través del tiempo, que les permitan desarrollarse, planear mejor su futuro, enfrentar imprevistos y disminuir riesgos.

En el 2020 Banco C contaba con 30 millones de cuentas y alrededor de 6.5 millones de créditos al consumo. Además, se ubicaba como el segundo en emisor de tarjetas de crédito, el tercero en emisor de tarjetas de débito y el quinto en red de cajeros automáticos¹. Al cierre del 2021, la cartera del banco ascendió a 32 mil 78 millones de pesos, lo que representó un aumento anual de 28.74 por ciento y el 0.58 por ciento del total crediticio del sector, según datos de la Comisión Nacional Bancaria y de Valores (CNBV).

En la actualidad, Banco C es una de las instituciones bancarias que más sucursales tiene en el país², con poco más de 1,200, sólo está por debajo de su competencia directa que cuenta con casi 2,000 sucursales, y el banco más longevo que cuenta con alrededor de 1,700 sucursales. Sin embargo, quiere digitalizar aún más sus procesos para ampliar y mejorar su atención a clientes de otros segmentos, pero sin descuidar la atención física. En el 2018, el 80% de transacciones totales que hacía el banco eran en ventanilla bancaria, y solamente 20% eran digitales, electrónicas y por otros canales. A la fecha de elaboración de este trabajo, casi el 60% ya son fuera de ventanilla y solamente, 40% son en ventanilla³.

¹ Muñoz, H. (2020, mayo 23). 13 años de Banco C y bancarización. El Sol de México. <https://www.elsoldemexico.com.mx/analisis/13-anos-de-bancol-y-bancarizacion-5266466.html>

² Economista, E. (2022, mayo 6). Banco C quiere ser un banco cada vez más digital. El Economista. <https://www.eleconomista.com.mx/sectorfinanciero/BanCo-quiere-ser-un-banco-cada-vez-mas-digital-20220505-0121.html>

³ Alavez, M. (2020, marzo 4). Nuestros clientes están contentos: Banco C. El Sol de México | Noticias, Deportes, Gossip, Columnas. <https://www.elsoldemexico.com.mx/finanzas/nuestros-clientes-estan-contentos-banco-4921803.html>

Por lo cual, la institución ha evolucionado conforme a lo que el cliente bancario ha ido demandando, a través de ofrecer servicios de mayor calidad y flexibilidad que requieren una inversión en tecnología y software para poder cumplir sus expectativas, por lo cual, Banco C tiene en su planeación estratégica realizar una inversión de más de 10,000 millones de pesos en los siguientes cuatro años⁴, simplemente en cuestiones tecnológicas, que tienen que ver con una experiencia multicanal donde se permite una interacción con el banco a través de distintos puntos de contacto, como, por ejemplo, a través de la página web y las aplicaciones del banco. Prueba de ello, es que su aplicación para teléfonos celulares cuenta ya con 4 millones de usuarios, y 97% de las transferencias a través del Sistema de Pagos Electrónicos Interbancarios (SPEI) se realiza por este canal⁵.

Finalmente, en lo que va de 2022, los segmentos con mayores avances son los préstamos personales y tarjetas de crédito⁶.

Misión

Ser el banco favorito para la gran mayoría del mercado popular, ofreciendo de la manera más fácil, productos financieros acordes a sus necesidades.

Visión

Ser el banco número uno de la clase popular mexicana en cuanto a la preferencia de clientes, servicio, atención, calidad y productos, reflejándose esta condición en el número de clientes del banco y obteniendo la más alta rentabilidad entre los bancos de este segmento, mediante el uso racional y prudente de los recursos.

⁴ Economista, E. (2022a, marzo 24). Banco C invertirá 10,000 mdp en tecnología en los próximos cuatro años. El Economista. <https://www.eleconomista.com.mx/sectorfinanciero/BanCo-invertira-10000-mdp-en-tecnologia-en-los-proximos-cuatro-anos-20220323-0149.html>

⁵ Economista, E. (2022, mayo 6). Banco C quiere ser un banco cada vez más digital. El Economista. <https://www.eleconomista.com.mx/sectorfinanciero/BanCo-quiere-ser-un-banco-cada-vez-mas-digital-20220505-0121.html>

⁶ Ensástigue, M. (2022, marzo 29). Banco C se moderniza con gran inversión. El Sol de México | Noticias, Deportes, Gossip, Columnas. <https://www.elsoldemexico.com.mx/finanzas/banco-se-moderniza-con-gran-inversion-8059285.html>

2. Objetivo.

El propósito de esta investigación es diseñar e implementar un modelo de Gestión de Incidentes basado en las mejores prácticas internacionales para el área de Seguridad de la Información del Banco C, que permita establecer procedimientos, actividades y métodos internos de gestión con la finalidad de reducir daños tanto reputacionales como económicos con los cuales se mantendría el objetivo del negocio el cual consiste en ser el banco número uno de la clase popular en cuanto a la preferencia de clientes, servicio, atención, calidad y productos.

Objetivos Particulares.

1. Crear una base de datos precisa con la información generada de los incidentes recurrentes reportados en el primer año de registro donde se pueda identificar las categorías
2. Identificar los tipos de subcategoría y niveles de priorización para la atención de los incidentes recurrentes en el primer año de registro.
3. Establecer una solución por cada subcategoría de los incidentes recurrentes del primer año que permitan ofrecer una adecuada atención y minimicen los tiempos de atención.

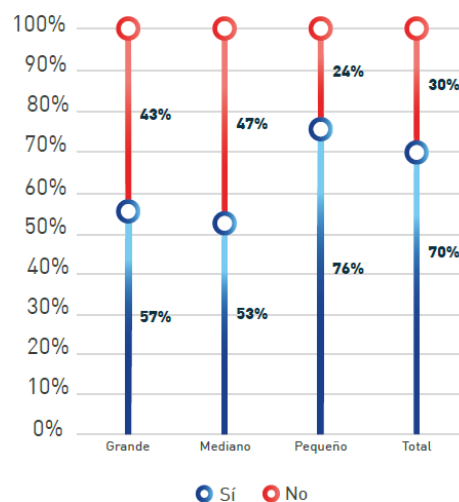
3. Antecedentes.

En el 2019, la Secretaría General de la Organización de los Estados Americanos (OEA), realizó un estudio llamado: Estado de Ciberseguridad en el Sistema Financiero Mexicano⁷, en el cual la información recolectada proviene de 240 entidades e instituciones financieras participantes del sistema Financiero Mexicano, con el fin de fortalecer las capacidades y el nivel de conciencia sobre las crecientes amenazas a la seguridad digital que aborda a la región.

Los hallazgos relevantes para esta investigación los encontramos en las siguientes gráficas que se formularon como parte de los resultados obtenidos del estudio, en el cual, entre los puntos destacables tenemos que:

En la mayoría de las instituciones financieras sin importar su tamaño, solo existe un área encargada de la seguridad de la información y fraudes digitales como la muestra en la gráfica 1.

Gráfica 1. Área única responsable de la seguridad digital en la entidad / institución financiera.

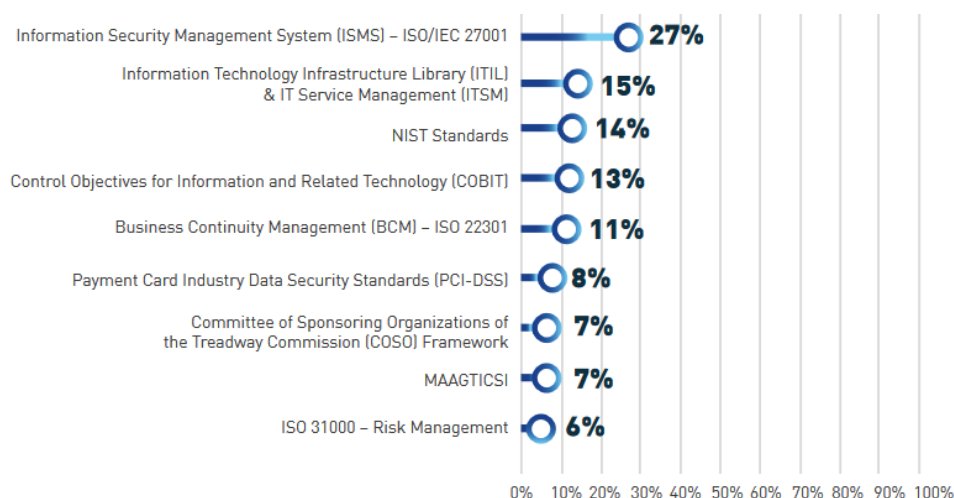


Nota: Tomado del Reporte -Estado de Ciberseguridad en el Sistema Financiero Mexicano. (2019)-.

Por otra parte, se resalta en la gráfica 2 el uso de la ISO 27001 como el marco y/o estándar internacional en torno a la seguridad de la información más usado por parte de las entidades e instituciones financieras del país.

⁷ Estado de Ciberseguridad en el Sistema Financiero Mexicano. (2019). <https://www.casede.org/index.php/biblioteca-casede-2-0/seguridad/ciberseguridad/648-estado-de-ciberseguridad-en-el-sistema-financiero-mexicano/file>

Gráfica 2. Marcos de seguridad y/o estándares internacionales adoptados.



Nota: Tomado del Reporte -Estado de Ciberseguridad en el Sistema Financiero Mexicano. (2019)-.

Además, podemos observar en la gráfica 3 que la Gestión de Incidentes de seguridad se encuentra en el lugar 9 de los programas implementados en las instituciones financieras del país más comunes asociados a la seguridad digital.

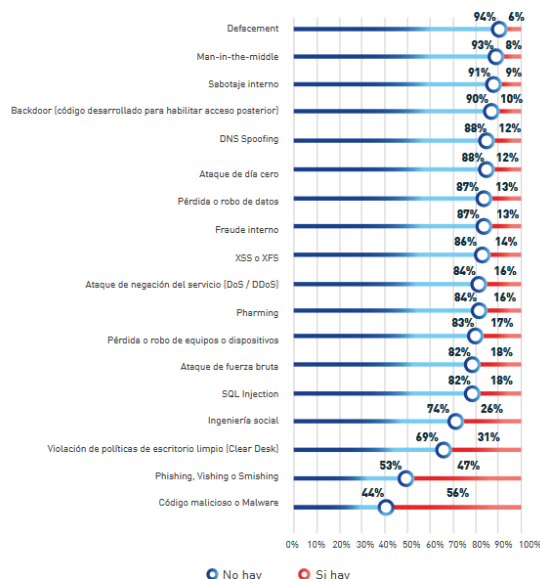
Gráfica 3. Procesos / programas respecto a la seguridad digital implementados actualmente por las entidades e instituciones financieras.



Nota: Tomado del Reporte -Estado de Ciberseguridad en el Sistema Financiero Mexicano. (2019)-.

Por otra parte, en la gráfica 4 podemos observar que el Phishing, Vishing o Smishing ocupan el segundo lugar de los eventos de seguridad digital más comúnmente identificados por las instituciones financieras

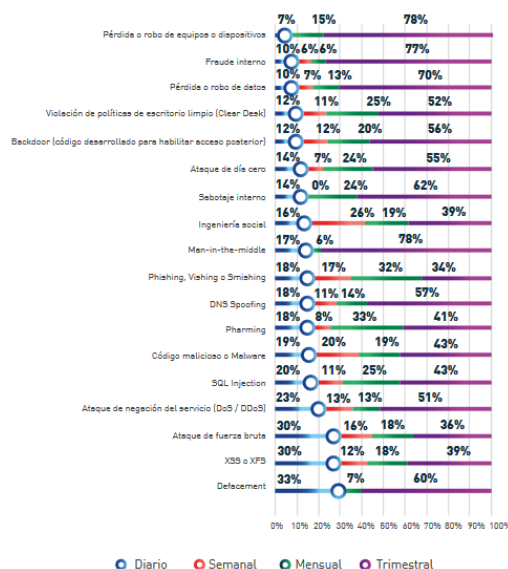
Gráfica 4. *Eventos (ataques exitosos y ataques no exitosos) de seguridad de la información contra las entidades e instituciones financieras que se han identificado durante los últimos doce meses.*



Nota: Tomado del Reporte -Estado de Ciberseguridad en el Sistema Financiero Mexicano. (2019)-.

Adicionalmente, se aprecia en la gráfica 5 que, con respecto al Phishing, Vishing o Smishing la frecuencia aproximada de ocurrencia de eventos un 18% de las entidades identifican ocurrencia de este tipo de eventos diariamente, un 17% del total lo identifican semanalmente, un 32% del total lo identifican mensualmente, y un 34% del total lo identifican trimestralmente.

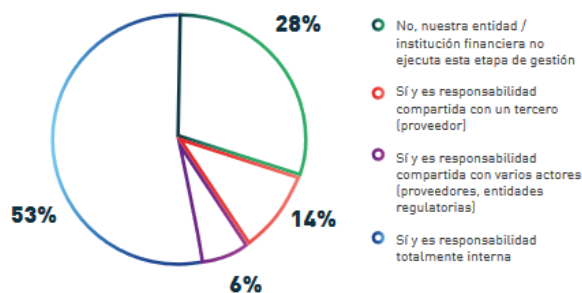
Gráfica 5 Frecuencia en la ocurrencia de eventos de seguridad de la información contra las entidades e instituciones financieras.



Nota: Tomado del Reporte -Estado de Ciberseguridad en el Sistema Financiero Mexicano. (2019)-.

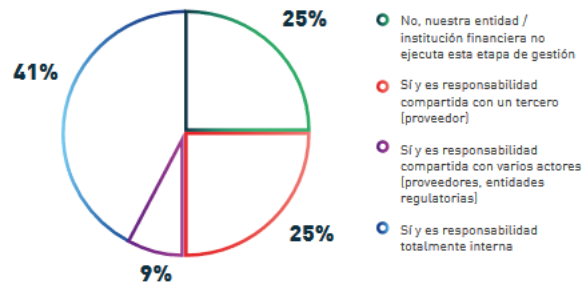
También, el estudio realizó un análisis de las etapas de gestión frente a incidentes de seguridad de la información donde se destaca que: en la etapa de priorización de incidentes el 53% de las entidades del país cuentan y ejecutan una estrategia (gráfica 6), el 41% de las entidades del país cuentan y ejecutan una estrategia de contención de incidentes (gráfica 7), con respecto a la respuesta de incidentes el 38% de las entidades del país cuentan y ejecutan una estrategia (gráfica 8), y el 42% de las entidades del país cuentan y ejecutan una estrategia de recuperación de incidentes bajo la responsabilidad interna de la organización (gráfica 9).

Gráfica 6 Estrategias de Priorización frente a incidentes de seguridad digital.



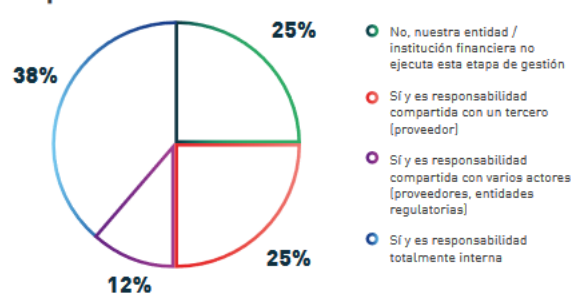
Nota: Tomado del Reporte -Estado de Ciberseguridad en el Sistema Financiero Mexicano. (2019)-.

Gráfica 7 Estrategias de Contención frente a incidentes de seguridad digital.



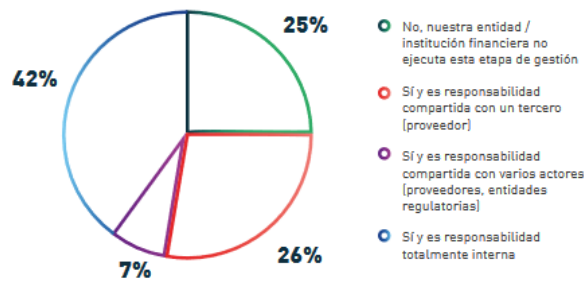
Nota: Tomado del Reporte -Estado de Ciberseguridad en el Sistema Financiero Mexicano. (2019)-.

Gráfica 8 Estrategias de Respuesta frente a incidentes de seguridad digital.



Nota: Tomado del Reporte -Estado de Ciberseguridad en el Sistema Financiero Mexicano. (2019)-.

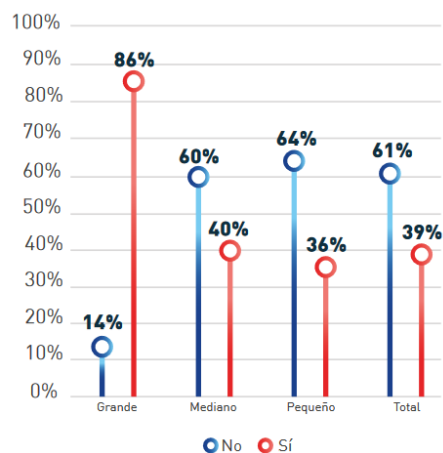
Gráfica 9 Estrategias de Recuperación frente a incidentes de seguridad digital.



Nota: Tomado del Reporte -Estado de Ciberseguridad en el Sistema Financiero Mexicano. (2019)-.

De igual manera, el estudio realiza la pregunta de qué si tiene la existencia de mecanismos para que sus clientes de servicios financieros reporten a la entidad incidentes de seguridad digital sufridos, mostrando que el 61% de total no lo tiene y esto varía según el tamaño de la entidad como se muestra en la gráfica 10.

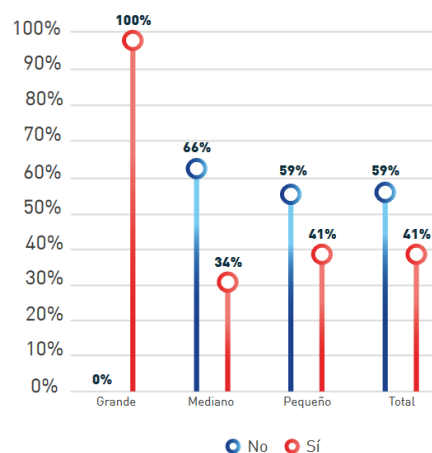
Gráfica 10 ¿La institución financiera ofrece un mecanismo para que sus de servicios financieros reporten incidentes de seguridad de la información (incluyendo ciberseguridad y fraudes ocurridos a través de medios digitales)?



Nota: Tomado del Reporte -Estado de Ciberseguridad en el Sistema Financiero Mexicano. (2019)-.

Continuando con las preguntas del reporte, se aprecia en la gráfica 11 las respuestas de si se cuenta con un plan de comunicaciones que permita informar a los clientes de servicios financieros cuando su información personal se haya visto comprometida, dónde se observa que en todas las entidades grandes existe un plan de comunicaciones para informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida.

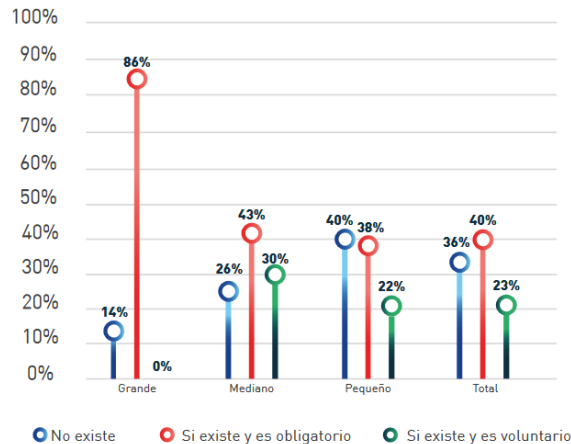
Gráfica 11 ¿La institución financiera a la cual usted pertenece cuenta con un plan de comunicaciones que permita informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida?



Nota: Tomado del Reporte -Estado de Ciberseguridad en el Sistema Financiero Mexicano. (2019)-.

En la gráfica 12 se observa que el 86% de las entidades grandes manifiestan que conocen algún mecanismo para reportar incidentes y es obligatorio debido a la existencia de disposiciones establecidas por alguna autoridad de regulación, mientras que las entidades medianas es el 43% y el 38% en las entidades pequeñas.

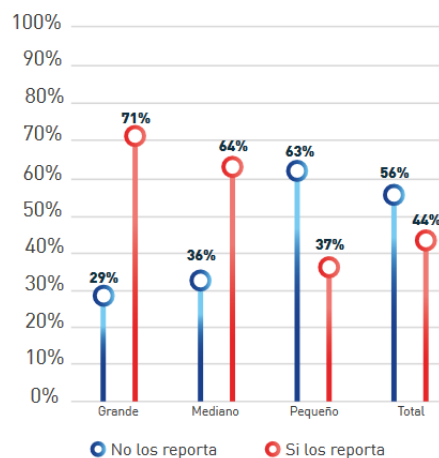
Gráfica 12 ¿Conoce algún mecanismo para reportar incidentes de seguridad de la información sufridos por la institución financiera a la cual usted pertenece ante una autoridad de regulación en México?



Nota: Tomado del Reporte -Estado de Ciberseguridad en el Sistema Financiero Mexicano. (2019)-.

Adicionalmente, para complementar las preguntas anteriores, la gráfica 12 muestra que el 71% de las entidades grandes, el 64% de las entidades medianas y el 37% de las entidades pequeñas reportan los incidentes sufridos ante una autoridad de procuración de justicia.

Gráfica 13 ¿La institución financiera a la cual usted pertenece reporta los incidentes de seguridad de la información sufridos ante una autoridad de procuración de justicia en México?



Nota: Tomado del Reporte -Estado de Ciberseguridad en el Sistema Financiero Mexicano. (2019)-.

4. Situación Actual.

En la actualidad, bastantes organizaciones utilizan estándares internacionales y marcos de referencia para sus operaciones en la gestión de incidentes de seguridad con la finalidad de buscar eficiencia en las soluciones y los tiempos de respuesta, optimizando los recursos y el talento humano de la organización. Como, por ejemplo, el proceso de incidentes de las mejores prácticas de ITIL, el marco principal de COBIT y el marco de trabajo que propone la ISO/IEC 27001.

No obstante, uno de los inconvenientes que enfrenta el responsable de la Seguridad de la Información en el Banco C es la gestión de incidentes de seguridad y sus riesgos asociados, ya que, carece de un modelo establecido de gestión de atención a incidentes que realice la investigación, recopilación, procesamiento y análisis de información que provenga de cualquier fuente relacionada con los productos y servicios que ofrece la Institución.

Este proceso inicia con la notificación de un SOC (Security Operation Center), el cual es el encargado de realizar un monitoreo en la Internet para encontrar un posible incidente de seguridad de la información que podría afectar al banco, después lo notifica al área de Seguridad de la Información del banco C, la cual primero registra el incidente y luego investiga con las demás gerencias cual podría atenderlo, y con esta notificación al área el proceso se cierra

En consecuencia, se genera una base de datos improvisada con los registros para llevar un seguimiento y control de los incidentes para que las Gerencias encargadas de resolución puedan tener información directa y precisa para evaluar y tomar las acciones correspondientes de resolución.

5. Problemática.

La ausencia de un modelo establecido de gestión de atención de incidentes en el Banco C ha generado que se tenga un registro improvisado de incidentes y soluciones, lo que genera que se incumpla con el artículo 168 bis 11 sección IX de la Circular Única de Bancos del Gobierno Mexicano, la cual menciona:

“Que para la atención de los Incidentes de Seguridad de la Información se cuente con procesos de gestión que aseguren la detección, clasificación, atención y contención, investigación y, en su caso, análisis forense digital, diagnóstico, reporte a niveles jerárquicos competentes, solución, seguimiento y comunicación a autoridades, clientes y contrapartes de dichos incidentes.

Para la detección y respuesta de Incidentes de Seguridad de la Información a que hace referencia el párrafo anterior, el director general deberá designar un equipo que incorpore a personal de las diferentes áreas de la Institución para participar en cada actividad del proceso de gestión antes señalado del que, en todo caso, deberá formar parte el oficial en jefe de seguridad de la información de conformidad con la fracción VII del Artículo 168 Bis 14 de estas disposiciones. (p. 348)”

Además, de que no existe una categorización y priorización de atención con respecto a la criticidad de los incidentes, por lo cual, el responsable de la Seguridad de la Información en el Banco C tiene una baja calidad de atención en su trabajo y surge un descontento en la alta dirección del Banco C por el mal servicio brindado, lo que ocasiona tener mala calidad e imagen por parte de la institución, generando desconfianza con los clientes.

Con esta investigación se ayudará a desarrollar un modelo de Gestión de atención de Incidentes basado en buenas prácticas internacionales en el sector bancario, para mejorar el nivel de gestión y control en el área de Seguridad de la Información. Además, de tener un enfoque estructurado y planificado que involucre a diferentes áreas en la propuesta de estrategia con la finalidad de reducir daños tanto reputacionales como económicos y que permita manejar adecuadamente los incidentes de seguridad de la información.

6. Desarrollo.

6.1 Desarrollo de modelo de gestión de incidentes

El Desarrollo del modelo consta de cuatro fases, las cuales son:

- Diseño de la Gestión de Incidente.
- Proceso de la Gestión del Incidente
- Actividades Post Incidentes
- Tratamiento para los incidentes recurrentes.

6.1.1 Fase 1: Diseño de la Gestión de Incidente.

6.1.1.1 Objetivo.

El Objetivo del área de Seguridad de la Información es proporcionar información detallada sobre el proceso de Gestión de Incidentes que desarrolla el área para todo el equipo involucrado. El proceso en sí permitirá conocer desde el registro de la ocurrencia hasta su solución y cierre

6.1.1.2 Políticas.

Se elaboró una política general de la Seguridad de la Información, donde se definió que el área de Seguridad de la Información será el único punto de contacto con terceros para el registro de incidentes. Además, de que todo incidente tendrá un área responsable y que el analista del área de Seguridad de la Información será el encargado de darle seguimiento hasta su solución y cierre, y documentará cada vez que se realice un cambio de estado. Esto ayudó a establecer el compromiso brindado por parte de la administración.

6.1.1.3 Definición de los roles y actividades del equipo de Trabajo.

El equipo de trabajo está conformado por los siguientes roles y actividades:

- **SOC:** Empresa o tercero responsable de:

- Buscar incidentes relacionados con el Banco C tanto en la Internet como en la Deep Web y Redes Sociales.
- Notificar los incidentes al Gestor de Incidentes.
- Dar atención a los incidentes.
- **Gestor de Incidentes:** Empleado del Banco C del área de Seguridad de la Información responsable de:
 - Registrar los incidentes.
 - Categorizar los incidentes.
 - Priorizar los incidentes.
 - Analizar y Evaluar los incidentes.
 - Asignar los incidentes al Soporte de 1° o 2° nivel para su atención.
 - Documentar el cierre.
 - Dar atención a los incidentes.
- **Atención 1er nivel:** Proveedor o Gerencia del Banco C responsable de:
 - Dar atención a los incidentes de seguridad de la información identificados con prioridad crítica y alta.
- **Atención 2° nivel:** Gerencia del Banco C responsable de:
 - Dar atención a los incidentes de seguridad de la información identificados con prioridad baja y media.

6.1.2 Fase 2: Proceso de la Gestión del Incidente.

En esta sección, se muestra el flujo de los procesos propuestos para la gestión de incidentes que se proponen para el área de Seguridad de la Información.

6.1.2.1 Reportar Incidente.

Cuando el SOC detecte, sospeche o conozca de la materialización de un incidente de seguridad de la información relacionado con el Banco C, deberá llenar el formato Reporte de Incidente y enviarlo por correo electrónico a la cuenta de correo del área de Seguridad de la Información.

Para el llenado de los reportes de los incidentes, el formato debe contar con la mayor cantidad y exactitud posible de información, a lo cual, se divide en cuatro secciones: encabezado del reporte, datos de quien reporta el incidente, información sobre el incidente y descripción del incidente, las cuales se describen a continuación:

a) Encabezado del reporte de incidentes:

- Fecha de reporte: Se debe escribir en formato DD/MM/AAAA (día, mes, año).
- Hora del reporte: Se debe escribir en formato HH:MM (hora, minutos).
- Folio del reporte: Se debe escribir en formato AAAA - Lugar - Folio (Año, Donde ocurrió el Incidente, Número de reporte consecutivo)
- Lugar del Incidente: Se debe escribir el lugar donde se encontró el incidente (Facebook, Twitter, Clear web, Cybersquatting, Telegram, Deep Web, Instagram, TikTok, Phishing, YouTube y WhatsApp)

b) Datos de quien reporta el incidente.

- Nombres: Nombre completo del tercero que realiza el reporte.
- Dependencia: Nombre del lugar donde labora el tercero que realiza el reporte.

c) Información sobre el incidente.

- Descripción del incidente: Breve descripción contestando las preguntas ¿Qué sucedió? ¿Cómo sucedió? y ¿Dónde sucedió?
- Recomendaciones: Breve descripción de posibles acciones a tomar.

6.1.2.2 Registrar el Incidente.

El Gestor de Incidentes responsable del Banco C realiza el registro inmediato correspondiente para cada reporte en la Base de Datos, de esta forma cuando se registra el incidente automáticamente también se registra la base de conocimiento. Para dar inicio al proceso debe registrar los siguientes datos:

- i. Folio del reporte.
- ii. Fecha de reporte.
- iii. Hora del reporte.
- iv. ¿Quién reporta?
- v. ¿Dónde sucedió?
- vi. ¿Qué sucedió?
- vii. Categoría.
- viii. Impacto.
- ix. Urgencia.
- x. Prioridad.
- xi. Acciones tomadas por S.I.
- xii. Área asignada.
- xiii. Estatus del folio (Abierto, En gestión, En investigación, Cerrado)
- xiv. Fecha de atención S.I.
- xv. Hora de atención S.I.
- xvi. Fecha de cierre.
- xvii. Acciones realizadas para el cierre.

6.1.2.3 Categorizar el Incidente.

La categorización del incidente tiene como objetivo principal el recopilar toda la información que pueda ser utilizada para la resolución de este. El proceso debe ser realizado por el Gestor de Incidentes y debe contar, al menos, con los siguientes elementos:

a) Categoría

- **Redes Sociales:** Medios creados para que las personas puedan compartir, en tiempo real, contenido escrito o visual con su grupo de amigos, familiares o conocidos a través de Internet⁸. (Facebook, Twitter, Instagram, TikTok, YouTube).
- **Clear Web:** Todas las páginas webs cuyo acceso está abierto para todo el mundo e indexado por los principales motores de búsqueda.⁹
- **Deep Web:** Es la parte de la web que no está indexado en los motores de búsqueda web. Esta web engloba todo aquello que estando en línea, no es público, sino oculto y con carácter privado.
- **Phishing:** Es una técnica que consiste en el envío de un correo electrónico en el que los ciberdelincuentes suplantan la identidad de entidades, y su objetivo es obtener toda la información personal y bancaria que puedan conseguir. Para ello, adjuntan archivos infectados o enlaces a páginas fraudulentas.¹⁰
- **Mensajería Instantánea:** Es un tipo de comunicación basada en texto, entre dos personas que tienen una conversación por medio de computadoras, tabletas, teléfonos inteligentes o cualquier dispositivo conectado a internet. (Telegram y WhatsApp).¹¹

⁸ (S/f). Platzi.com. Recuperado el 18 de septiembre de 2022, de <https://platzi.com/clases/2314-terminos-marketing-digital/39800-que-son-las-redes-sociales-y-para-que-usarlas/>

⁹ Bree, P. (2019, diciembre 6). Tecnología empresarial: ¿Qué son la Clear Web, la Deep Web y la Dark Web? https://www.elespanol.com/invertia/disruptores-innovadores/innovadores/tecnologicas/20191206/tecnologia-empresarial-clear-web-deep-dark/449706519_0.html

¹⁰ ¿Qué es el phishing? (s/f). Osi.es. Recuperado el 18 de septiembre de 2022, de <https://www.osi.es/es/actualidad/blog/2021/11/17/que-es-el-phishing>

¹¹ Quiroz, A. (2022, febrero 7). ¿Qué es y para qué sirve la mensajería instantánea? B2Chat. <https://www.b2chat.io/blog/mensajeria-instantanea/mensajeria-instantanea-tipos-para-que-sirve/>

b) Sub-Categoría:

- **Código:** Archivos con las instrucciones necesarias, realizadas en un lenguaje de programación, que sirve para compilar posteriormente un programa o aplicaciones de la entidad.
- **Cybersquatting:** Es la apropiación de nombres de dominio, consiste en registrar un determinado nombre de dominio que simula a uno legítimo, para posteriormente traficar con él o hacer uso con fines fraudulentos.¹²
- **Daño reputacional:** Quejas sobre los servicios ofrecidos por la entidad.
- **Fraude de trámite de crédito:** Productos ofrecidos en publicaciones de redes sociales fuera de los procesos establecidos por la entidad.
- **Información expuesta de posibles clientes:** Datos de tarjetas de supuestos clientes de la entidad.
- **Sitios Web Phishing:** Son copias falsas de los sitios web de la entidad de modo que pide introducir credenciales y/o datos bancarios.
- **Phishing en redes sociales:** Enlaces a páginas fraudulentas encontradas en redes sociales.
- **Sitios con información no autorizada:** Páginas Web con información confidencial de la entidad.
- **Smishing en redes sociales:** Quejas de usuarios de redes sociales sobre mensajes de texto donde se le pide que entren a un sitio web fraudulento.
- **Suplantación de identidad:** Redes sociales que se hacen pasar por las redes oficiales de la entidad.

¹² Cybersquatting, qué es y cómo protegerse. (2019, febrero 7). INCIBE. <https://www.incibe.es/protege-tu-empresa/blog/cybersquatting-y-protegerse>

6.1.2.4 Priorización del Incidente.

Para evaluar la priorización que tendría que asignar el Gestor de Incidentes si los incidentes se materializaran, se desarrollaron características o criterios que ayudan a determinar el nivel que se tendría. Con este fin se elabora una matriz de cálculo de prioridades, y los factores a evaluar son el impacto y la urgencia del incidente:

- **Impacto:**

Determina la importancia del incidente de seguridad de la información dependiendo de la afectación a los clientes y la entidad. Los niveles de impacto se describen a continuación en la tabla 1:

Tabla 1. Categorías de Impacto de Incidentes.

Categorías	Valor	Descripción
Crítico	4	Daño catastrófico a la reputación con cobertura a nivel nacional y de forma prolongada; intervención regulatoria con sanciones por faltas muy graves; pérdida de clientes a gran escala; involucramiento directo de la alta gerencia.
Alto	3	Daño reputacional mayor, investigación del regulador y sanciones por falta grave; involucramiento de la alta gerencia, gran cantidad de clientes afectados; pérdidas financieras mayores.
Medio	2	Daño reputacional medio, pocos clientes afectados, existen sanciones por falta leve.
Bajo	1	No hay impacto directo, no hay daño a la reputación, no existen sanciones legales ni impacto financiero u operacional; no es percibido por los clientes, pero si por los colaboradores

Nota: Elaboración propia.

- **Urgencia:**

Depende del tiempo máximo de demora para la resolución del incidente. Las categorías definidas para la urgencia se detallan en la Tabla 2:

Tabla 2. Categorías de Urgencia de Incidentes.

Categorías	Valor	Descripción
Alto	3	El daño causado por el incidente aumenta rápidamente con el tiempo.
Medio	2	El daño causado por el incidente aumenta considerablemente con el tiempo.
Bajo	1	El daño causado por el incidente sólo aumentó marginalmente con el tiempo.

Nota: Elaboración propia.

Luego de tener definidas las variables se obtiene la prioridad mediante la siguiente formula: $\text{Prioridad} = \text{Impacto} * 0.25 + \text{Urgencia} * 0.25$ y con el resultado se determinará la valoración del incidente y su nivel de prioridad de atención mediante la siguiente tabla 3:

Tabla 3. Determinación del nivel de prioridad.

Rango	Escala	Tiempo de Respuesta
1.75 - 2	Crítica	Inmediato
1.5 - 1.74	Alta	4 horas.
1 - 1.49	Media	12 horas.
0 - 0.99	Baja	24 horas.

Nota: Elaboración propia.

Con base al resultado de la evaluación del nivel de prioridad del incidente, se indica su valoración de la siguiente manera:

- **Crítica:** La atención es inmediata y prioritaria.
- **Alta:** Puede esperar hasta 4 horas para su atención.
- **Media:** Puede esperar hasta 12 horas para su atención.
- **Baja:** Puede esperar hasta 24 horas para su atención.

Así mismo, los tiempos de respuesta fueron asignados para estar dentro de las 48 horas que la regulación mexicana pide en el artículo 168 Bis 16 sección II de la Circular Única de Bancos del Gobierno Mexicano, la cual menciona:

“Cuando el Incidente de Seguridad de la Información refiera a que la Información Sensible que se encuentre en custodia de la Institución o de terceros que le presten servicios, fue extraída, extraviada, eliminada, alterada o bien, las Instituciones sospechen de la realización de algún acto que involucre accesos no autorizados a dicha información, el director general o la persona que este designe, deberán notificar a los clientes la posible pérdida, extracción, alteración, extravío o acceso no autorizado a su información, dentro de las siguientes 48 horas a que ocurrió el Incidente de Seguridad de la Información o a que se tuvo conocimiento de este, a través de los medios de notificación que el cliente haya señalado para tal efecto, a fin de prevenirlo de los riesgos derivados del mal uso de la información que haya sido extraída, extraviada, eliminada, o alterada,

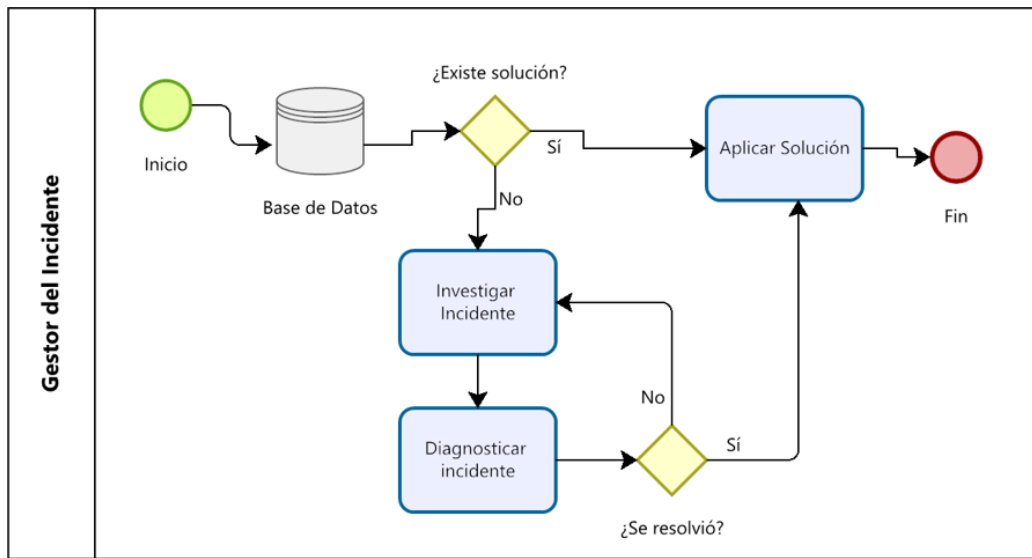
debiendo informarle las medidas que deberá tomar y, en su caso, efectuar la reposición de los medios de disposición que correspondan o la sustitución de Factores de Autenticación necesarios. La evidencia de esta notificación deberá incluirse en el resultado de la investigación señalada en el párrafo anterior.”

6.1.2.5 Investigación y Diagnóstico del Incidente.

El Gestor del Incidente deberá investigar, diagnosticar y documentar todas las actividades. Una vez identificada la solución, deberá probarse adecuadamente con atención de 1° o 2° nivel, dependiendo el caso, garantizando que la atención sea la óptima. El flujo que deberá seguir es el siguiente que se muestra en la imagen1:

- i. Buscar en la BD si existe una solución temporal o definitiva para el incidente.
- ii. ¿Existen solución en la BD?
 - No: Continúa con proceso.
 - Sí: Fin del proceso.
- iii. Investigar y diagnosticar.
- iv. ¿Incidente diagnosticado?
 - No: Volver al proceso.
 - Sí: Continúa con proceso.
- v. Fin del proceso.

Imagen 1. Actividades del Gestor de Incidentes.



Nota: Elaboración propia.

El Proceso de investigación y diagnóstico se considera finalizado cuando se ha diagnosticado el Incidente y el Gestor del Incidente ha identificado todos los síntomas del incidente y determinando exactamente que está mal y como corregirlo.

6.1.2.6 Solución y Documentación del Incidente.

Cuando una solución ha sido identificada debe ser aplicada por las gerencias que estarán implicadas en la toma de acciones de atención. Los pasos necesarios para resolver el incidente son los siguientes:

- i. Asignar el incidente a la gerencia responsable de ejecutar las soluciones temporales o definitivas.
- ii. Actualizar el estado del incidente.
- iii. Registrar la solución del incidente en la BD.
- iv. Solicitar evidencia a las gerencias responsable de ejecutar las soluciones.
- v. Adjuntar documento al incidente.
- vi. Cerrar incidente.

El proceso de solución, recuperación y documentación se considera finalizado cuando se ha solucionado el Incidente y se ha registrado la solución.

6.1.3 Fase 3: Actividades Post Incidentes.

6.1.3.1 Lecciones aprendidas.

El Gestor de Incidentes llevará el listado y análisis de los incidentes de seguridad de la información presentados durante el periodo, así como, las actividades que se muestran a continuación:

- Mantener la documentación de los incidentes de seguridad de la Información.
- Crear bases de datos de conocimientos.
- Realizar capacitaciones a los empleados de la entidad en lo relacionado a incidentes de seguridad de la información.
- Analizar los hechos y tomar decisiones.

6.1.3.2 Uso de evidencias recolectadas.

Las evidencias recolectadas de incidentes de seguridad de la información deben ser almacenados para futuras investigaciones e implementación de controles de mejoramiento. La información que debe ser almacenada y custodiada por el Gestor de Incidentes incluye:

- Cantidad de incidentes tratados.
- Tiempo asignado a los incidentes.
- Daños ocasionados.
- Cantidad de activos de información involucrados.
- Frecuencia de incidentes.
- Pérdidas.

6.1.4 Fase 4: Tratamiento para los incidentes recurrentes.

El objetivo es consolidar las soluciones de acuerdo con las lecciones aprendidas que dejaron los incidentes de seguridad de la información que hayan ocurrido más de una vez y cuya importancia sea significativa para la entidad.

6.1.4.1 Soluciones basadas en las categorías de los incidentes.

Con base en la Subcategoría de los Incidentes de Seguridad de la Información mostrada en el punto 6.1.2.3, respecto al tratamiento de incidentes recurrentes se recomienda:

- Identificar posibles soluciones que eliminen o controlen las causas que dieron origen a este tipo de incidentes.
- Documentar de forma clara las soluciones que se implementen, con el fin de ser consultadas posteriormente.
- Realizar revisiones posteriores para garantizar que las soluciones implementadas hayan surtido los efectos esperados.

6.2 Herramientas de Soporte.

Los equipos de incidentes se deben hacer valer con herramientas, personas y las mejores prácticas o normas internacionales. No obstante, algunas herramientas son específicas para la gestión de incidentes, mientras que otras son herramientas más generales que el equipo utiliza también para otras tareas, por lo que para este el modelo del trabajo se sugiere utilizar alguna de las siguientes herramientas:

6.2.1 ServiceNow.

Permite la creación y asignación automática de incidentes, notificaciones, seguimiento de SLA, informes y ofrece espacios de trabajo de agentes visuales e intuitivos. Además, el producto cubre un conjunto completo de funciones de gestión de incidentes como lo son: Administración de incidentes, Informes y cuadros de mando, Gestión de problemas y Gestión del nivel de servicio

Pros:

- Alojado en la nube.
- Informes claros.
- Implementación sencilla.
- Sistema de gestión de tickets.

Contras:

- Alto costo inicial.
- Sin opción local.

6.2.2 Freshservice.

Es un sistema completo que permite administrar, supervisar e interactuar con cualquier incidente que ocurra dentro de las operaciones de la empresa. Permite manejar las consultas de los clientes, indexar incidentes y acelerar la prestación de servicios por lo que mantiene los datos seguros y completamente automatizados. Es simple y fácil de usar y desempeña un papel vital en el análisis y la resolución de problemas.

Pros:

- Escalabilidad.
- Seguridad.
- Gran base de recursos.
- Equipo orientado.

Contras:

- Enfocado en atender a una base de clientes internos.
- Falta de integraciones de redes sociales.

6.2.3 Mesa de servicio de JIRA.

Es una solución para equipos pequeños y medianos que permite la notificación, la gestión de tickets y la comunicación en toda la empresa de forma optimizada. Está orientado a minimizar posibles interrupciones e incidentes al proporcionar un excelente sistema de indexación, información y análisis relativamente detallados.

Pros:

- Fácil de usar.
- Ligerero.
- Interfaz de usuario amigable.
- Notificaciones de toda la empresa.

Contras:

- Carece de funciones que son básicamente parte de los estándares de la industria.
- Relativamente caro.

6.2.4 OpsGenie.

Es una popular herramienta de gestión de incidentes basada en la nube. Proporciona una solución para organizaciones de pequeña y gran escala ya que el servicio es una opción principal si se desea centralizar los tickets, informes de incidentes e interrupciones en un solo lugar para que se puedan resolver, indexar y rastrear correctamente. Además, ayuda a planificar y prepararse para incidentes determinando a quién responder, qué plantilla usar, cómo colaborar y también creando una página de estado.

Pros:

- Solución completa.
- Alertas e informes dinámicos.
- Funciones de priorización.
- Múltiples canales de notificación.

Contras:

- Privilegios de administrador mediocres.
- Programación compleja.

6.2.5 LiveAgent.

Ofrece una gama de soluciones completas, como la ubicación centralizada para almacenar tickets, la automatización del servicio al cliente, la gestión de incidentes y las alertas. Además, esta herramienta de gestión de incidentes permitirá los flujos de trabajo de automatización y gestión de tickets más completos y complejos.

Pros:

- Fácil de usar.
- Asequible.
- SaaS Cloud software.

Contras:

- Sin integración de WhatsApp y LinkedIn.

7. Resultados.

7.1 Flujo de trabajo.

El siguiente capítulo introduce las actividades realizadas para comprobar que los objetivos específicos planteados en el capítulo 2 logren satisfacer los indicadores de logro mencionados. Para lo cual, se propone las cuatro etapas del ciclo de Deming (Plan, Do, Check, Act).

- **Plan.**

En esta fase se mencionan al Personal y las actividades que realizará.

- **Ejecución.**

En esta fase se da ejecución al plan seleccionado.

- **Resultados.**

En esta fase se revisan los resultados obtenidos de las pruebas realizadas.

- **Plan de Mejora.**

Esta fase puede ser usado como un ciclo de mejora continua donde se proponen mejoras respecto a los objetivos específicos analizados.

7.2 Objetivo: Crear una base de datos precisa con la información generada de los incidentes reportados.

En este punto se realizará una base de datos con los incidentes recurrentes reportados durante el primer año.

7.2.1 Plan.

Para crear una base de datos precisa con la información generada de los incidentes reportados, el Gestor de Incidentes deberá realizar una base de datos con la información recolectada del primer año de los incidentes que fueron recurrentes, tomando en cuenta el punto 6.1.2.2 Registrar el Incidente, además, de realizar la categorización de estos incidentes recurrentes conforme al punto 6.1.2.3 Categorizar el Incidente.

7.2.2 Ejecución.

Se registró en una tabla de Excel los incidentes recurrentes reportados por el equipo SOC como se muestra en la tabla 4, la cual contiene todos los puntos para el levantamiento de información de incidentes como se menciona en el punto 6.1.2.2 Registrar el Incidente.

Tabla 4. Campos relacionados a la apertura de incidentes.

Folio del Reporte	Fecha de reporte	Hora del reporte	¿Quién reporta?	¿Dónde sucedió?	¿Qué sucedió?	Categoría	Impacto	Urgencia	Prioridad	Acciones tomadas por SI	Área asignada	Estatus del folio	Fecha de atención SI	Hora de atención SI	Fecha de cierre	Acciones realizadas para el cierre

Nota: Elaboración propia.

Además, con base a los incidentes registrados durante el primer año, se obtuvo el total de incidentes que fueron recurrentes de acuerdo con su categoría establecida en el punto 6.1.2.3 Categorizar el Incidente y que se muestran a continuación en la tabla 5.

Tabla 5. Número de Incidentes por categoría en el primer año.

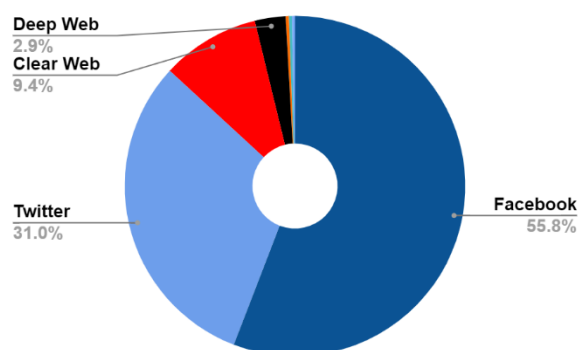
¿Dónde sucedió?	Total
Facebook	191
Twitter	106
Clear Web	32
Deep Web	10
TikTok	1
Telegram	1
Instagram	1

Nota: Elaboración propia.

7.2.3 Resultados.

Al realizar el análisis de la gráfica 14, se evidencia que hay categorías donde se concentran la mayoría de las incidencias, de las cuales Facebook y Twitter concentran más del 85%, mientras que la Clear Web y la Deep Web no representan ni el 15% restante.

Gráfica 14. *Porcentaje de Incidentes por categoría en el primer año.*



Nota: Elaboración propia.

7.2.4 Plan de Mejora.

Debido a que el primer año no obtuvo una atención adecuada para registrar los incidentes de seguridad de la información, para el plan de mejora se consideró el segundo año para poder contar con un registro de incidentes más acertado y poder complementar la base de conocimientos, los resultados se muestran en la tabla 6.

Tabla 6. *Número de Incidentes por categoría al segundo año.*

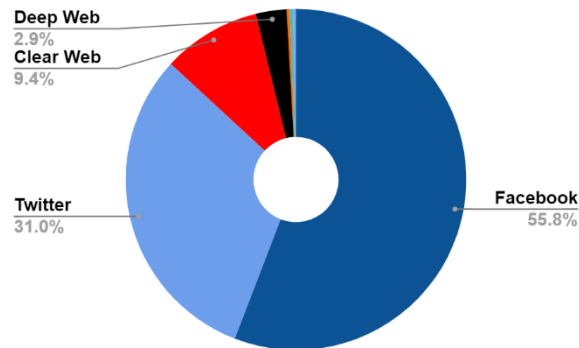
¿Dónde sucedió?	Total
Facebook	736
Twitter	496
Clear Web	291
Phishing	290
Telegram	97
Deep Web	35
Instagram	18
YouTube	4
WhatsApp	1
TikTok	1

Nota: Elaboración propia.

De esta forma, como se ve en la gráfica 15, se tiene una gama amplia de categorías, en la cual Facebook y Twitter disminuyen su porcentaje de recurrencias y se tiene nuevas categorías

en las cuales se debe poner atención como lo son el Phishing con el 14.7% y Telegram con el 4.9%.

Gráfica 15. *Porcentaje de Incidentes por categoría al segundo año.*



Nota: Elaboración propia.

7.3 Objetivo: Identificar los tipos de subcategoría y niveles de priorización para la atención de los incidentes.

En este punto se realizó la clasificación por subcategoría y niveles de priorización para la atención de los incidentes recurrentes.

7.3.1 Plan.

Se toma en consideración las categorías establecidas en el punto 7.2.4 de los casos recurrentes al segundo año, para que el Gestor de Incidentes en este plan pueda realizar las subcategorías para luego establecer los niveles de priorización de los incidentes con base en el punto 6.1.2.4 Priorización del Incidente.

7.3.2 Ejecución.

Se realizó la subcategorización conforme al punto 6.1.2.3 Categorizar el Incidente y obtuvo el total de casos como se muestra en la tabla 7.

Tabla 7. *Número de Incidentes por subcategoría al segundo año.*

Categoría	Total
Daño reputacional	472
Fraude de trámite de crédito	432
Sitios Web Phishing	291
Suplantación de identidad	255
Cybersquatting	229
Información expuesta de posibles clientes	196
Smishing en redes sociales	41
Phishing en redes sociales	32
Sitios con información no autorizada	17
Código	4

Nota: Elaboración propia.

Después de haber obtenido la representación de incidentes recurrentes por subcategoría, se procedió a asignarles un valor e impacto de acuerdo con el punto 6.1.2.4 Priorización del Incidente, y se ve en la Tabla 8:

Tabla 8. *Impacto de Incidentes por subcategoría.*

Categoría	Impacto	Valor
Sitios Web Phishing	Critico	4
Información expuesta de posibles clientes	Critico	4
Código	Critico	4
Suplantación de identidad	Alto	3
Fraude de trámite de crédito	Medio	2
Smishing en redes sociales	Medio	2
Phishing en redes sociales	Medio	2
Sitios con información no autorizada	Medio	2
Daño reputacional	Bajo	1
Cybersquatting	Bajo	1

Nota: Elaboración propia.

Así mismo, como se ve en la tabla 9, se le asignó una urgencia a cada subcategoría.

Tabla 9. Urgencia de Incidentes por subcategoría.

Categoría	Urgencia	Valor
Sitios Web Phishing	Alta	3
Información expuesta de posibles clientes	Alta	3
Código	Alta	3
Suplantación de identidad	Media	2
Fraude de trámite de crédito	Media	2
Smishing en redes sociales	Media	2
Phishing en redes sociales	Media	2
Sitios con información no autorizada	Media	2
Daño reputacional	Baja	1
Cybersquatting	Baja	1

Nota: Elaboración propia.

Finalmente, utilizando la formula del punto 6.1.2.4 Priorización del Incidente, se obtuvo la prioridad de atención y tiempos de respuesta de acuerdo con lo establecido y como se muestra en la tabla 10.

Tabla 10. Prioridad de atención por subcategoría.

Categoría	Prioridad	Tiempo de Respuesta
Sitios Web Phishing	Crítico	Inmediato
Información expuesta de posibles clientes	Crítico	Inmediato
Código	Crítico	Inmediato
Suplantación de identidad	Medio	12 horas
Fraude de trámite de crédito	Medio	12 horas
Smishing en redes sociales	Medio	12 horas
Phishing en redes sociales	Medio	12 horas
Sitios con información no autorizada	Medio	12 horas
Daño reputacional	Bajo	24 horas
Cybersquatting	Bajo	24 horas

Nota: Elaboración propia.

7.3.3 Resultados.

A realizar la asociación de categoría con subcategoría obtenemos la tabla 11, en la cual podemos ver que Facebook, Twitter y Clear Web ocupan los primeros 3 lugares al tener la mayor cantidad de subcategorías.

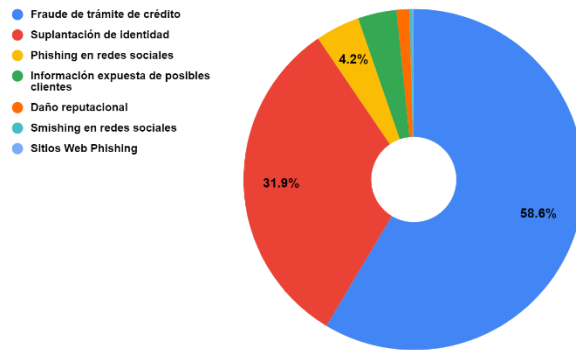
Tabla 11. Asociación de Categorías con subcategoría.

Categoría	Subcategoría	Total
Facebook	Fraude de trámite de crédito	431
	Suplantación de identidad	235
	Phishing en redes sociales	31
	Información expuesta de posibles clientes	27
	Daño reputacional	9
	Smishing en redes sociales	2
	Sitios Web Phishing	1
Twitter	Daño reputacional	456
	Smishing en redes sociales	38
	Suplantación de identidad	1
	Phishing en redes sociales	1
Clear Web	Cybersquatting	229
	Información expuesta de posibles clientes	38
	Sitios con información no autorizada	16
	Daño reputacional	4
	Código	4
Phishing	Sitios Web Phishing	290
Telegram	Información expuesta de posibles clientes	96
	Fraude de trámite de crédito	1
Deep Web	Información expuesta de posibles clientes	35
Instagram	Suplantación de identidad	18
YouTube	Daño reputacional	2
	Suplantación de identidad	1
	Sitios con información no autorizada	1
WhatsApp	Smishing en redes sociales	1
TikTok	Daño reputacional	1

Nota: Elaboración propia.

Por otra parte, al separar las 3 categorías con mayor cantidad de subcategorías como lo fueron Facebook, Twitter y Clear Web, se puede observar en las siguientes gráficas que, en Facebook, el 80% está constituido por las categorías de fraude de trámite de crédito y suplantación de identidad

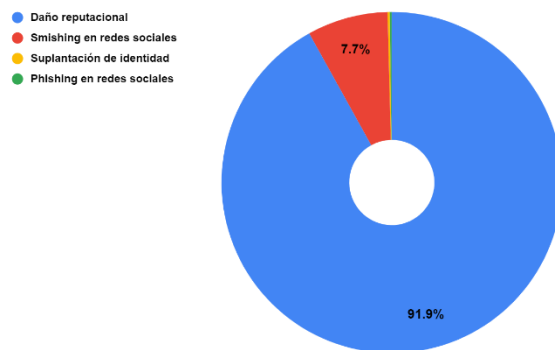
Gráfica 16. *Subcategorías de Facebook.*



Nota: Elaboración propia.

Así mismo, en Twitter la subcategoría que más domina es el daño reputacional con el 91.9% seguido del smishing en redes sociales con el 7.7% como se muestra en la gráfica 17.

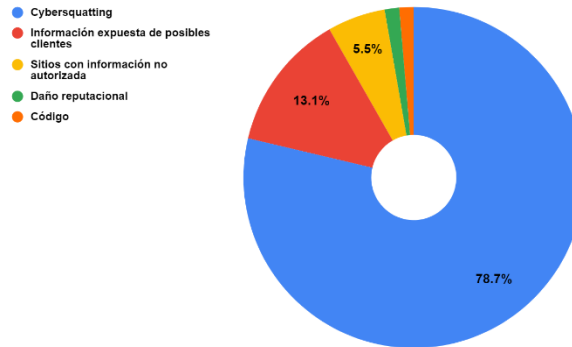
Gráfica 17. *Subcategorías de Twitter.*



Nota: Elaboración propia.

Mientras que, en la Clear Web, el cybersquatting fue la subcategoría que más domino con el 78.7% seguido con la información expuesta de posibles clientes con el 13.1% como se ve en la gráfica 18.

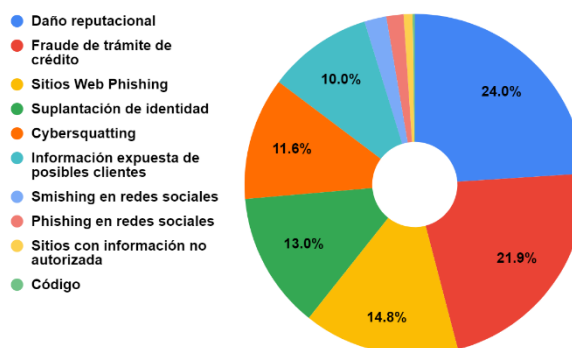
Gráfica 18. *Subcategorías de Clear Web.*



Nota: Elaboración propia.

Por otra parte, como se puede observar en la gráfica 19, al sacar el total de la subcategorización de los incidentes recurrentes de los dos primeros años, se obtiene una visión más detallada de lo que está afectando al Banco C, como, por ejemplo, el daño reputacional representa el 24%, mientras que el fraude de trámite de crédito es el 21%, los sitios web phishing el 14.8% y la suplantación de identidad con el 13%.

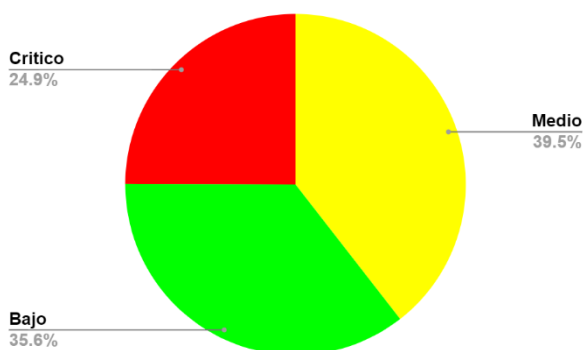
Gráfica 19. *Porcentaje de los incidentes a los primeros años por subcategoría.*



Nota: Elaboración propia.

Por otro lado, como se muestra en la gráfica 20, podemos observar que los incidentes categorizados como Medios son los que han sido mayores con un 39.5%, seguidos de los categorizados como Bajo con 35.6% y Críticos con el 24.9%.

Gráfica 20. Porcentaje por prioridad de los incidentes.



Nota: Elaboración propia.

7.3.4 Plan de Mejora.

Debido a que en la prioridad Alta no apareció en la valoración inicial de urgencia de incidentes, se tuvo que realizar una nueva valorización de la Urgencia como se muestra en la tabla 12, para poder obtener un nuevo nivel de atención a los incidentes quedando de la siguiente forma:

Tabla 12. Nueva valorización de Urgencia de Incidentes por subcategoría.

Categoría	Urgencia	Valor
Sitios Web Phishing	Alta	3
Información expuesta de posibles clientes	Alta	3
Código	Alta	3
Suplantación de identidad	Alta	3
Fraude de trámite de crédito	Media	2
Smishing en redes sociales	Media	2
Phishing en redes sociales	Media	2
Sitios con información no autorizada	Media	2
Daño reputacional	Baja	1
Cybersquatting	Baja	1

Nota: Elaboración propia.

Y la tabla 13 muestra como quedo la Prioridad de atención de los incidentes:

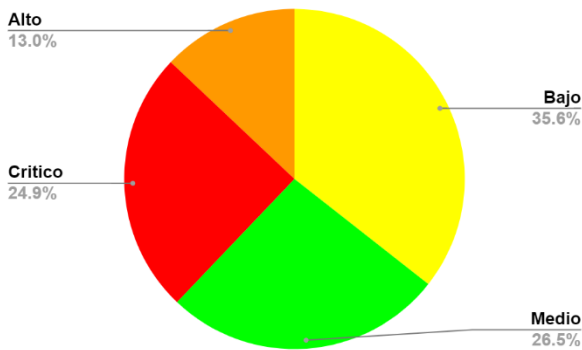
Tabla 13. Nueva Prioridad de atención por subcategoría.

Categoría	Prioridad	Tiempo de Respuesta
Sitios Web Phishing	Crítico	Inmediato
Información expuesta de posibles clientes	Crítico	Inmediato
Código	Crítico	Inmediato
Suplantación de identidad	Alta	4 horas
Fraude de trámite de crédito	Medio	12 horas
Smishing en redes sociales	Medio	12 horas
Phishing en redes sociales	Medio	12 horas
Sitios con información no autorizada	Medio	12 horas
Daño reputacional	Bajo	24 horas
Cybersquatting	Bajo	24 horas

Nota: Elaboración propia.

Por lo cual, el porcentaje de prioridad de incidentes cambia como se muestra en la gráfica 21 y nos da el nivel de atención deseado; el de prioridad alta con un 13%, lo que hace que el bajo quede en 35.5%, medio con 26.5% y el crítico con el 24.9%, lo que genera que se pueda atender los incidentes en diferentes intervalos de tiempo.

Gráfica 21. Nuevo porcentaje por prioridad de los incidentes.



Nota: Elaboración propia.

7.4 Objetivo: Establecer una solución por cada subcategoría de los incidentes recurrentes.

En este punto es donde se procede a asignar una solución para dar atención por cada subcategoría de los incidentes recurrentes.

7.4.1 Plan.

Conforme a la subcategorización del punto anterior, el Gestor de Incidente deberá asignar a un responsable de 1° o 2° nivel, además, de establecer una solución de atención.

7.4.2 Ejecución.

Con base a la subcategorización y prioridad asignada en el punto anterior, se dio una propuesta de atención conforme al punto 6.1.2.5 Investigación y Diagnóstico del Incidente, en la cual, tomando los incidentes recurrentes de los primeros años, el flujo de atención quedo como se muestra en la tabla 14:

Tabla 14. Atención de incidentes por subcategoría.

Categoría	Pasos	Acciones realizadas para el cierre	Área asignada
Sitios Web Phishing	1	Comprobar si es un sitio valido	SI
	2	Notificar al área asignada que trámite la baja del sitio	SI
	3	Tramitar la baja del sitio	SOC
Información expuesta de posibles clientes	1	Comprobar si son tarjetas de clientes del banco	SI
	2	Notificar al área asignada que trámite la baja de las tarjetas	SI
	3	Tramitar la baja de las tarjetas	Fraudes
	4	Avisar al cliente del reemplazo	Fraudes
Código	1	Solicitar la revisión del código	SI
	2	Notificar al área asignada que trámite la baja del sitio	SI
	3	Validar si es código del banco	Sistemas
	4	Tramitar la baja del sitio donde se almacena	SOC
Suplantación de identidad	1	Comprobar si es una red social valida	SI
	2	Tramitar la baja con la red social correspondiente	SI
	1	Revisar los perfiles y publicaciones	SI

Fraude de trámite de crédito	2	Tramitar la baja con la red social correspondiente	SI
Smishing en redes sociales	1	Notificar al área asignada para dar atención	SI
	2	Dar atención al usuario de la red social	EC
	3	Notificar al área asignada que trámite la baja del sitio	SI
	4	Tramitar la baja del sitio	SOC
Phishing en redes sociales	1	Notificar al área asignada para dar atención	SI
	2	Dar atención al usuario de la red social	EC
	3	Notificar al área asignada que trámite la baja del sitio	SI
	4	Tramitar la baja del sitio	SOC
Sitios con información no autorizada	1	Comprobar si es un sitio valido	SI
	2	Notificar al área asignada que trámite la baja del sitio	SI
	3	Tramitar la baja del sitio	SOC
Daño reputacional	1	Notificar al área asignada para dar atención	SI
	2	Dar atención al usuario de la red social	EC
Cybersquatting	1	Notificar al área asignada para dar atención	SI
	2	Notificar al área asignada que trámite la baja del sitio	SI
	3	Realizar campaña de concientización mencionando los sitios validos	EC
	4	Monitorear los sitios para cuando se activen	SOC

Nota: Elaboración propia.

De esta manera, teniendo identificado a las áreas asignadas para la atención de incidentes y su prioridad de atención, se asigna la atención de 1° y 2° nivel, quedando como se muestra en la tabla 15:

Tabla 15. Niveles de incidentes por subcategoría.

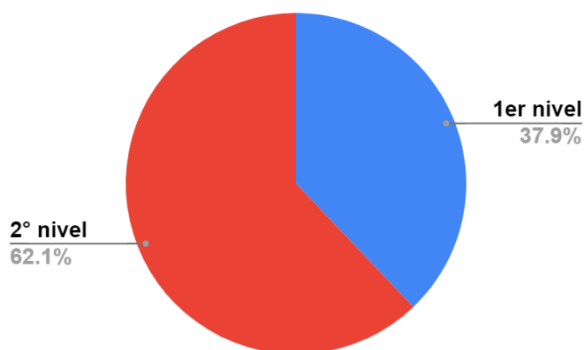
Categoría	Prioridad	Área asignada	Atención
Sitios Web Phishing	Crítico	SOC	1er nivel
Información expuesta de posibles clientes	Crítico	Fraudes	1er nivel
Código	Crítico	Sistemas	1er nivel
Suplantación de identidad	Alta	Seguridad de la Información	1er nivel
Fraude de trámite de crédito	Medio	Seguridad de la Información	2° nivel
Smishing en redes sociales	Medio	Experiencia del Cliente	2° nivel
Phishing en redes sociales	Medio	Experiencia del Cliente	2° nivel
Sitios con información no autorizada	Medio	SOC	2° nivel
Daño reputacional	Bajo	Experiencia del Cliente	2° nivel
Cybersquatting	Bajo	Experiencia del Cliente	2° nivel

Nota: Elaboración propia.

7.4.3 Resultados.

Con base al punto anterior, se obtuvo el total de incidentes recurrentes de los niveles de atención, de esta manera, podemos observar en la gráfica 22 que la atención de 2° nivel representa el 62.1% mientras que el 1er nivel el 37.9%.

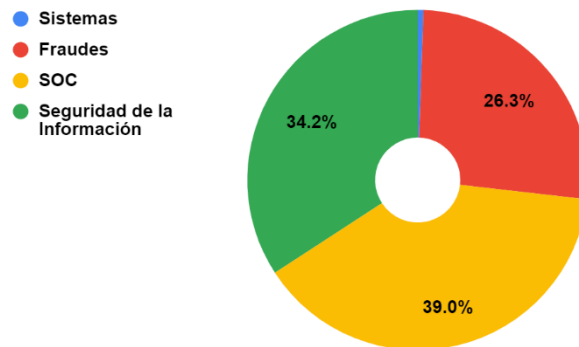
Gráfica 22. Porcentaje de incidentes por niveles de atención.



Nota: Elaboración propia.

Ahora, si se mira a profundidad a las áreas, podemos observar en la gráfica 23 que el SOC atiende la mayoría de los incidentes de 1er nivel con el 39%, mientras que Seguridad de la Información atiende el 34.2% y Fraudes el 26.3%.

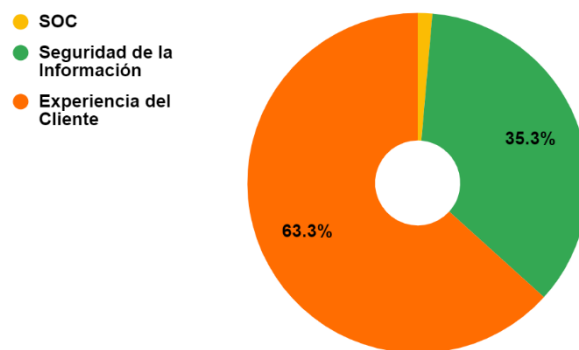
Gráfica 23. Porcentaje de atención de 1er nivel por áreas.



Nota: Elaboración propia.

Por otra parte, cuando se hace la revisión por atención de 2° nivel, se puede observar en la gráfica 24 que el área de Experiencia del Cliente atiende la mayoría de los incidentes con el 63.3%, seguido de Seguridad de la Información con el 35.3 y el SOC con el 1.4%.

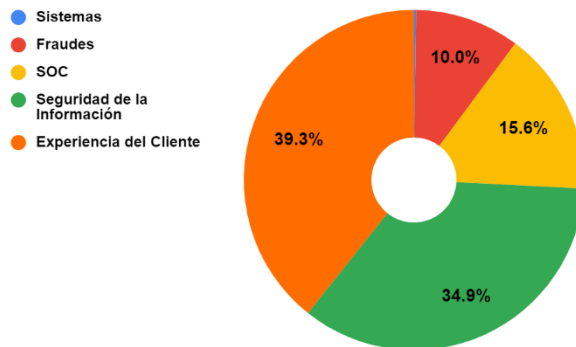
Gráfica 24. Porcentaje de atención de 2° nivel por áreas.



Nota: Elaboración propia.

Finalmente, en la gráfica 25 se puede observar que las áreas que más incidentes atienden son la de experiencia del cliente con el 39.3%, seguido de Seguridad de la Información con el 34.9%.

Gráfica 25. *Porcentaje de incidentes atendidos por área.*



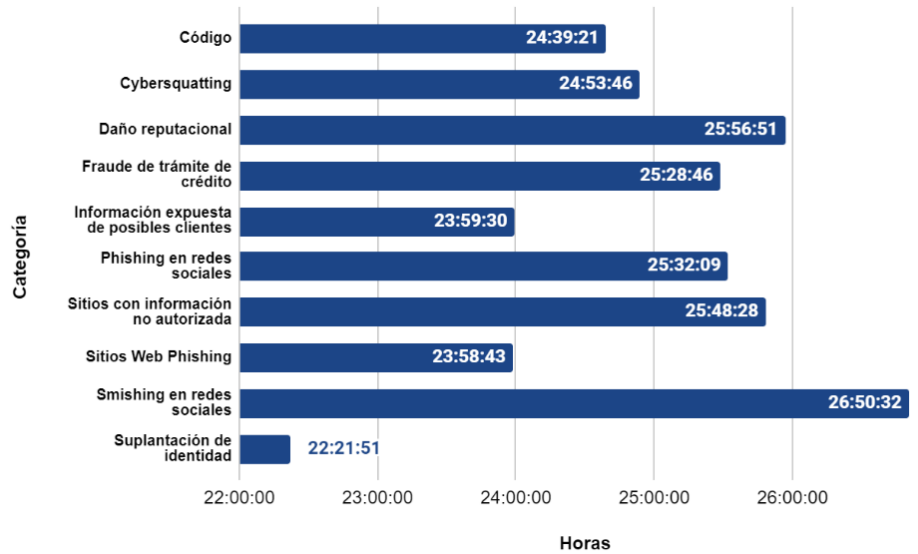
Nota: Elaboración propia.

7.4.4 Plan de Mejora.

El plan de mejora en este punto fue realizar la comprobación de que los tiempos de atención hayan disminuido con respecto a los primeros incidentes.

Los tiempos de atención sin haber establecido el proceso de Gestión de atención de incidentes tenía un promedio de entre 22 hasta 27 horas dependiendo de la categoría establecida y como se puede ver en la gráfica 26.

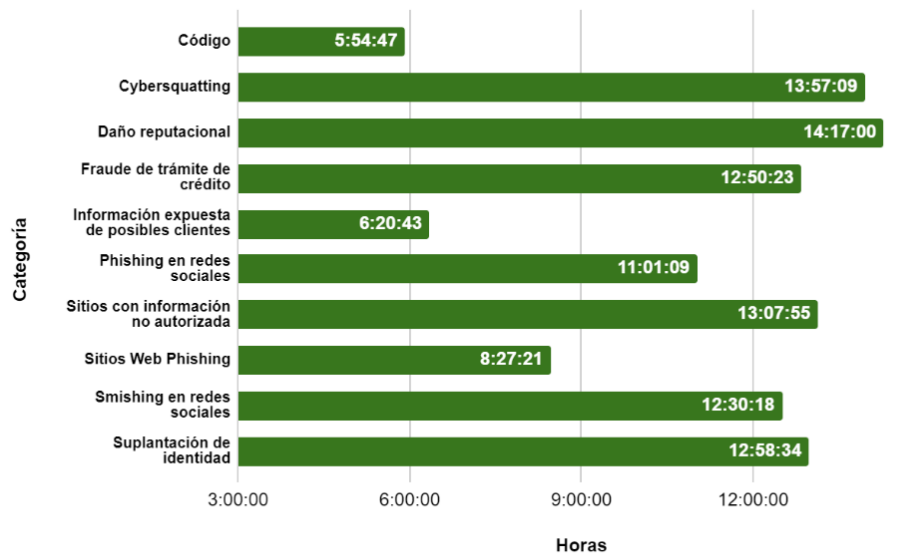
Gráfica 26. Promedio de horas para la atención de incidentes por categoría.



Nota: Elaboración propia.

Ahora bien, al implementar el modelo de gestión de incidentes, los tiempos de atención quedaron en promedio entre 5 hasta 14 horas como se puede observar en la gráfica 27.

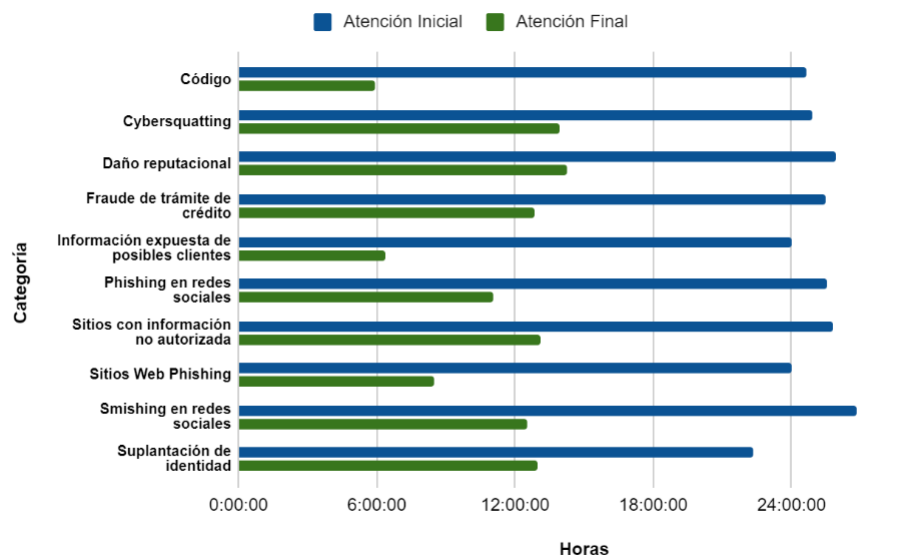
Gráfica 27. Promedio de horas para la atención de incidentes por categoría después del modelo.



Nota: Elaboración propia.

A continuación, se puede observar que, al establecer el modelo de gestión de incidentes con su categorización y prioridad, se reduce el promedio para la atención como en el caso de los incidentes considerados como críticos y altos, los cuales se redujeron hasta más del 50% como se muestra en la gráfica.

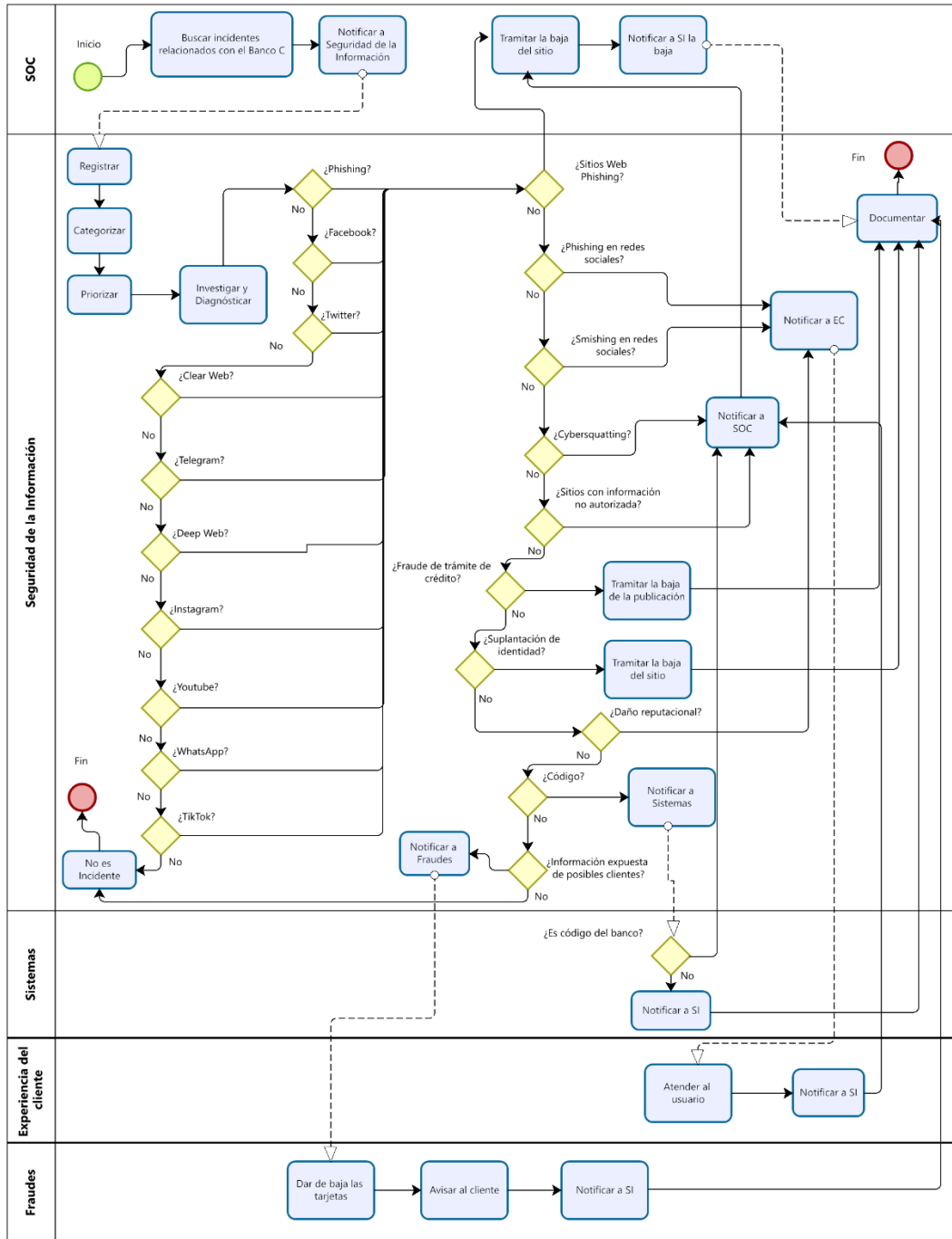
Gráfica 28. Comparación del promedio de horas para la atención de incidentes por categoría antes y después del modelo de gestión de incidentes.



Nota: Elaboración propia.

Finalmente, se realiza un diagrama con todas las actividades que se deben hacer para llevar cabo la Gestión de Incidentes de seguridad de la información y se muestra en la imagen siguiente:

Imagen 2. Actividades para la Gestión del Incidente.



Nota: Elaboración propia.

8. ANALISIS DE RESULTADOS.

En este capítulo se recapitulan las soluciones planteadas para el modelo de Gestión de Incidentes basado en las mejores prácticas internacionales para el área de Seguridad de la Información del Banco C, resumiendo los avances logrados en cada una de las etapas del proyecto.

- I. Se diseñó un modelo de Gestión de Incidentes para establecer objetivos, políticas, además de roles y actividades del equipo de trabajo.
- II. Se establecieron procesos para la Gestión de Incidentes, en las cuales se describen las actividades que deben realizarse, como lo son: reportar, registrar, categorizar, priorizar, investigar y diagnosticar, además de, solucionar y documentar del incidente.
- III. Se identificaron algunas herramientas específicas para la gestión de incidentes, principalmente aquellos que podrían adaptarse para el modelo establecido de Gestión de Incidentes.
- IV. Se implementó el modelo de Gestión de Incidentes según los alcances establecidos al comienzo del proyecto. En primer lugar, se creó una base de datos con la información generada de los incidentes reportados durante los primeros años, lo cual permitió establecer la categoría. Una vez identificadas las categorías, se realizó la clasificación por subcategoría y niveles de priorización para la atención de los incidentes. Finalmente, se asignó una solución para dar atención por cada subcategoría de los incidentes recurrentes.

9. CONCLUSIONES.

- I. De acuerdo con los resultados obtenidos en este trabajo, se puede concluir que, al adaptar el modelo de gestión de incidentes de seguridad de la información a las necesidades de la institución basado en las mejores prácticas internacionales, nos ayudó para reducir daños tanto reputacionales como económicos. Además, de que su implementación se logró gracias a que se diseñó una política para la institución en la que se establecían procedimientos, actividades y métodos internos, las cuales, establecieron los lineamientos que los trabajadores de la institución deben seguir en sus labores diarias y que las áreas involucradas tenían que reportar.
- II. Por otra parte, un punto a favor de la base de datos improvisada que se tenía es que, al limpiarla, ayudó a crear la base de datos precisa para gestionar eficientemente los incidentes de seguridad de la información.
- III. Al mismo tiempo, esta base de datos creada y en conjunto con el modelo de gestión de incidentes de seguridad de la información, ayudo a establecer la categorización y priorización de acuerdo con las necesidades de atención de incidentes de la institución
- IV. Finalmente, la consecuencia de establecer la categorización y priorización fue que facilitó a encontrar soluciones de atención con mayor eficiencia y rapidez a los incidentes de seguridad de la información. Además, de que redujo hasta un 50% los tiempos de atención. Así mismo, las propuestas diseñadas en este documento se alinean a los recursos que están al alcance del Banco C y que no implican un esfuerzo considerable para su implementación. El éxito de la estrategia planteada depende en gran medida del compromiso adquirido por las personas que lleven a cabo el plan estratégico, no obstante, es necesario invertir en herramientas y personas con la misma energía y entusiasmo que se brinda al desarrollar productos y servicios a la comunidad que forma parte del mercado meta.

9. Referencias.

(S/f). Platzi.com. Recuperado el 18 de septiembre de 2022, de <https://platzi.com/clases/2314-terminos-marketing-digital/39800-que-son-las-redes-sociales-y-para-que-usarlas/>

¿Qué es el phishing? (s/f). Osi.es. Recuperado el 18 de septiembre de 2022, de <https://www.osi.es/es/actualidad/blog/2021/11/17/que-es-el-phishing>

Alavez, M. (2020, marzo 4). Nuestros clientes están contentos: Banco C. El Sol de México | Noticias, Deportes, Gossip, Columnas. <https://www.elsoldemexico.com.mx/finanzas/nuestros-clientes-estan-contentos-banco-4921803.html>

Bree, P. (2019, diciembre 6). Tecnología empresarial: ¿Qué son la Clear Web, la Deep Web y la Dark Web? https://www.lespanol.com/invertia/disruptores-innovadores/innovadores/tecnologicas/20191206/tecnologia-empresarial-clear-web-deep-dark/449706519_0.html

Csizmadia, A. (2021, August 10). *25 mejores softwares de gestión de incidentes*. LiveAgent; Quality Unit, LLC. <https://www.liveagent.es/blog/mejores-software-gestion-incidencias/>

Cybersquatting, qué es y cómo protegerse. (2019, febrero 7). INCIBE. <https://www.incibe.es/protege-tu-empresa/blog/cybersquatting-y-protegerse>

DOF - Diario Oficial de la Federación. (n.d.). Gob.mx. Retrieved July 2, 2023, from https://www.dof.gob.mx/nota_detalle.php?codigo=5544804&fecha=27/11/2018

Economista, E. (2022, mayo 6). Banco C quiere ser un banco cada vez más digital. El Economista. <https://www.eleconomista.com.mx/sectorfinanciero/BanCo-quiere-ser-un-banco-cada-vez-mas-digital-20220505-0121.html>

Economista, E. (2022a, marzo 24). Banco C invertirá 10,000 mdp en tecnología en los próximos cuatro años. El Economista. <https://www.eleconomista.com.mx/sectorfinanciero/BanCo-invertira-10000-mdp-en-tecnologia-en-los-proximos-cuatro-anos-20220323-0149.html>

Ensástigue, M. (2022, marzo 29). Banco C se moderniza con gran inversión. El Sol de México | Noticias, Deportes, Gossip, Columnas. <https://www.elsoldemexico.com.mx/finanzas/banco-se-moderniza-con-gran-inversion-8059285.html>

Estado de Ciberseguridad en el Sistema Financiero Mexicano. (2019). <https://www.casede.org/index.php/biblioteca-casede-2-0/seguridad/ciberseguridad/648-estado-de-ciberseguridad-en-el-sistema-financiero-mexicano/file>

Guevara, E. P. A. (2020). Plan estratégico para establecer un Gobierno Corporativo que permita la colocación exitosa de una empresa familiar en el mercado de valores de México. Universidad La Salle.

Instituto Colombiano de Normas Técnicas y Certificación. Código de buenas prácticas para controles de seguridad de la información. NTC- ISO/IEC 27002. Bogotá: ICONTEC, 2013. 64 48 p.

Jorge Eliécer González Díaz, V. A. P. R. (2016). Guía de Gestión de Incidentes de Seguridad de la Información para la oficina de tecnología de la información y la comunicación – OTCI del Ministerio de Salud y Protección Social, tomando como base la norma ISO 27001:2013. Universidad Piloto de Colombia.

MINTIC. (2016, junio 11). Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones. https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Modelo de gestión de incidencias de TI basado en ITIL y COBIT para generar valor al negocio <https://docplayer.es/79990104-Modelo-de-gestion-de-incidencias-de-ti-basadoen-til-y-cobit-para-generar-valor-al-negocio.html>

Muñoz, H. (2020, mayo 23). 13 años de BanCo y bancarización. El Sol de México. <https://www.elsoldemexico.com.mx/analisis/13-anos-de-banco-y-bancarizacion-5266466.html>

Quiroz, A. (2022, febrero 7). ¿Qué es y para qué sirve la mensajería instantánea? B2Chat. <https://www.b2chat.io/blog/mensajeria-instantanea/mensajeria-instantanea-tipos-para-que-sirve/>

Vara-Horna, Arístides (2010). ¿Cómo hacer una tesis en ciencias empresariales? Una guía efectiva para los estudiantes de administración, negocios internacionales, marketing, logística y recursos humanos. Instituto de Investigación de la Facultad de Ciencias Administrativas y Recursos Humanos. Lima. Manual electrónico disponible en internet.