PLAN DE CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN PARA EL BANCO MUNDO MUJER DE LA CIUDAD DE POPAYÁN PARA PRIMER SEMESTRE DE 2018.

NELFFY PAOLA VELASCO ORDOÑEZ

UNIVERSIDAD DEL CAUCA

FACULTAD DE CIENCIAS CONTABLES ECONÓMICAS Y

ADMINISTRATIVAS

ADMINISTRACIÓN DE EMPRESAS

POPAYÁN

2018

PLAN DE CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN PARA EL BANCO MUNDO MUJER DE LA CIUDAD DE POPAYÁN PARA PRIMER SEMESTRE DE 2018.

NELFFY PAOLA VELASCO ORDOÑEZ

ASESOR ACADÉMICO:

ESP. JORGE ERNESTO PÉREZ

ASESOR EMPRESARIAL:

CEO. JUAN PABLO RODRÍGUEZ.

UNIVERSIDAD DEL CAUCA

FACULTAD DE CIENCIAS CONTABLES ECONÓMICAS Y ADMINISTRATIVAS

ADMINISTRACIÓN DE EMPRESAS

POPAYÁN

2018

DEDICATORIA

A Dios por darme la sabiduría y disponer todo para alcanzar este logro, a ti toda la gloria; a mis padres y hermanos por su apoyo constante y motivación cada día.

AGRADECIMIENTOS

A Dios por prestarme la vida y permitirme este logro, a mi familia por ser inspiración constante cada día en mi carrera, especialmente a mi madre Ana Dolly Ordoñez por creer en mí siempre y darme el amor más incondicional que he conocido, al mejor compañero que la vida me obsequio, Angelo David Peña por su particular forma de aportar en mi trabajo, su motivación en todo momento y por las palabras que me impulsaron a no rendirme, a mis compañeros del área de Riesgos del BMM por contribuir a mi crecimiento profesional y personal, finalmente a mi apreciado asesor académico Jorge Ernesto Pérez, por ser una bendición desde el principio, y contribuir siempre con la mejor disposición a la realización de este trabajo.

A USTEDES INFINITAS GRACIAS, LOS AMO.

TABLA DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

No existe ninguna duda de que los delitos cibernéticos representan una gran amenaza para las organizaciones de hoy en día, quienes basan su éxito o innovación en información única y valiosa, que los hace competitivos. El sector financiero es un área de la economía en la cual las instituciones que lo conforman manejan y gestionan información que requiere de alto niveles de seguridad interna y externa de cada organización, lo que convierte tanto a la información como al talento humano, en activos de gran valor para la organización.

En consecuencia con lo anterior, el Banco Mundo Mujer ha establecido desde la vicepresidencia de riesgos un sistema General de Seguridad de la Información, que incluye las metodologías, políticas, manuales de procesos, y diferentes componentes para asegurar la confidencialidad, integridad y disponibilidad de la información; sin embargo, este sistema requiere de la estructuración de un Plan de Capacitación y Sensibilización en Seguridad de la Información, que permita mitigar constantemente los riesgos asociados a la información, generando también un compromiso permanente del talento humano frente a la protección y el buen uso de los activos de información de la organización.

El trabajo de practica responde a la necesidad descrita y se compone de V capítulos, el capítulo I incluye la contextualización del trabajo, en él se describe el problema a abordar y se plantean los objetivos principales del trabajo; el capítulo II está compuesto de la contextualización teórica, en el que se incluye el marco teórico, marco contextual, marco legal y el marco conceptual; en el capítulo III sobre la contextualización metodológica, se describe la metodología utilizada para el desarrollo del trabajo de práctica; el capítulo IV incluye el desarrollo de la práctica empresarial y finalmente en el capítulo V se exponen las conclusiones y sugerencias.

1. CONTEXTUALIZACIÓN DEL TRABAJO

1.1 PROBLEMATIZACIÓN

1.1.1 Descripción del problema

El Banco Mundo Mujer, organización del sector financiero basa principalmente sus operaciones en el manejo diario de gran cantidad de información de clientes y terceros, esto representa diversos riesgos asociados a la seguridad de la información que para el Banco se pueden materializar en pérdidas y afectación de los objetivos del negocio.

El Banco mundo mujer desde su temprana constitución como entidad bancaria (año 2015) cuenta con un Sistema General de Seguridad de la información (SGSI), en el cual se estipulan políticas, procesos, y manuales asociados a la seguridad de la información, sin embargo esto no es suficiente para mitigar los riesgos de seguridad de la información que son cada vez más evidentes.

Con la finalidad de mitigar estos riesgos y asegurar la confidencialidad integridad y disponibilidad de la información se hace necesario estructurar dentro del SGSI un Plan de Capacitación y Sensibilización en seguridad de la información dirigido a todos los colaboradores del banco.

1.1.2 Definición del problema

Debido a la importancia que la seguridad de la información representa para una organización y en especial para aquellas que hacen parte del sector financiero, para las cuales se evidencia una continua situación de riesgos que puede llegar afectar de manera significativa su normal funcionamiento; se plantea el siguiente interrogante:

¿Cómo mitigar los riesgos asociados a la seguridad de la información para el Banco mundo mujer?

1.2 JUSTIFICACIÓN

Existen varias razones que sustentan la necesidad de estructurar un Plan de Capacitación y Sensibilización en S.I; en primer lugar por los ataques cibernéticos de terceros, "según la superintendencia financiera (noviembre, 2017) más de 540.000 ataques cibernéticos se producen cada día en el país y según un estudio especializado de la firma Digiware, en Colombia en el último año se han presentado más de 197 millones de fraudes cibernéticos (…) De estos, 39,56 % son contra el sector financiero," (El Tiempo, Septiembre 2017).

En segundo lugar, porque la Seguridad de la información no solo puede verse vulnerada por ciberataques o fraudes cibernéticos, sino que pueden existir fugas internas de información , las cuales provienen directamente de sus colaboradores, tomando gran importancia la prevención de estas fugas; la fuga de información es el principal temor de las empresas latinoamericanas en materia de seguridad informática, según revelan los datos recopilados por el ESET Latinoamérica, Laboratorio de Investigación que cuentan con especialistas de seguridad, quienes anualmente elaboran el Eset Security Report, un documento que busca mostrar cuál es el panorama de seguridad de las empresas en toda la región.

Según ESET Latinoamérica para el año 2012 las mayores preocupaciones en SI por parte de las empresas se centraba en temáticas como el malware, fraude interno y fraude externo, como se evidencia en la figura 1, para el año 2017 el malware continua siendo la mayor preocupación (56%), seguida por la vulnerabilidad del software y sistemas (52%) y el Phishing (27%), tal como se ilustra en la figura 2.

Con base en lo anterior, es claro que el sector bancario se encuentra frente a varios retos relacionados con la seguridad de la información, según ASOBANCARIA, asociación representativa del sector financiero Colombiano, entre los 5 Retos para la prevención del fraude electrónico en Colombia 2018, se encuentra, la capacitación constante del personal "Es necesario que se prepare constantemente al personal sobre las últimas modalidades de fraude para que estén en capacidad de detectar archivos adjuntos sospechosos y verificar los dominios de páginas web, inclusive las que aparentemente corresponden a entes gubernamentales que envían información "oficial" " (ASOBANCARIA, 2017).

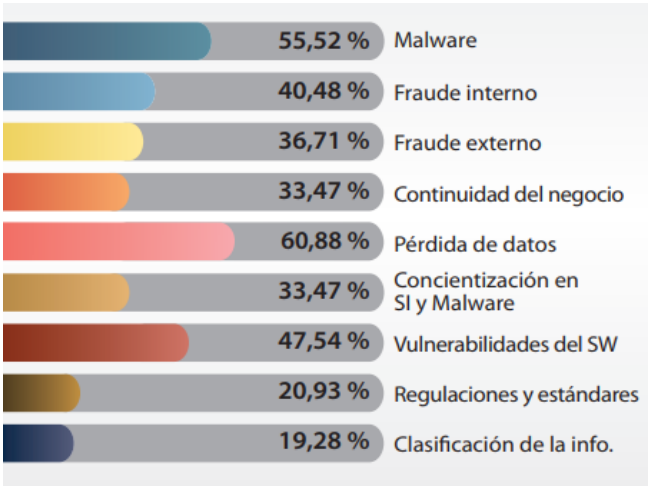


Figura 1. Mayores Preocupaciones en Seguridad de La Información en Las Empresas de Latinoamérica
Fuente: Fuente ESET Security Report Latinoamérica 2012

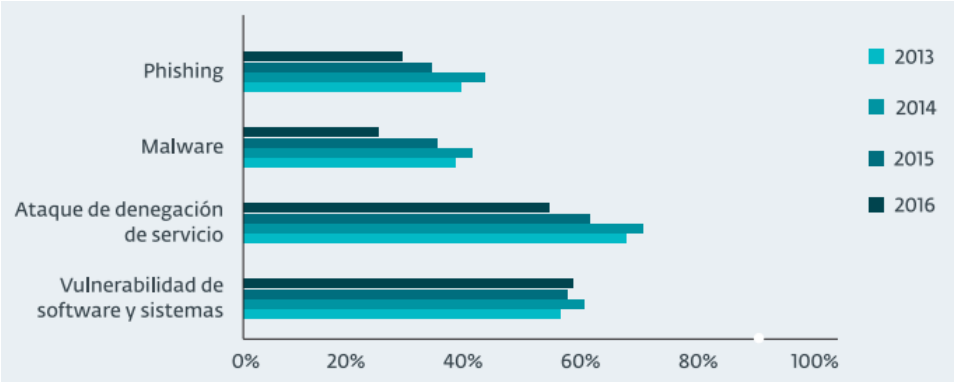


Figura 2. Principales Preocupaciones Respecto a la Seguridad de La Información en las Empresas de Latinoamérica
Fuente: Fuente ESET Security Report Latinoamérica 2017

El plan de capacitación y sensibilización para el BMM, es una herramienta valiosa, orientada en el rol fundamental que cumplen los usuarios y su educación como factor diferencial para garantizar la seguridad de la información. La razón por la cual es necesario elaborar este plan no solo se enfoca a las necesidades del sector financiero como tal, sino que adicionalmente desde la parte interna del área se han evidenciado riesgos inherentes a la seguridad de información, como el préstamo de contraseñas por parte de los colaboradores, el poco conocimiento sobre cómo hacer frente a ataques cibernéticos, el manejo inadecuado de información valiosa y la protección de los privilegios y accesos a la información.

Es importante resaltar que la elaboración de este plan de capacitación y sensibilización, permite poner en práctica muchos de los conocimientos adquiridos a lo largo de la carrera de administración de empresas, que giran en torno a los 4 principios básicos, la planeación, organización, dirección y control, que con el apoyo académico del Docente Jorge Ernesto Pérez, dan como resultado un mejor trabajo de práctica profesional.

Finalmente la elaboración de un plan de capacitación y sensibilización busca impactar de manera positiva en la organización Banco Mundo Mujer, proporcionando los lineamientos para la capacitación de los colaboradores y la sensibilización de los colaboradores, contribuyendo así a la disminución de los riesgos asociados a la seguridad de la información.

1.3 OBJETIVOS

1.3.1 Objetivo general

Elaborar el plan de capacitación y sensibilización en seguridad de la Información para Banco Mundo Mujer de la ciudad de Popayán, para el primer semestre de 2018.

1.3.2 Objetivos específicos

- Conocer los principales procesos y políticas del área de seguridad de la información.
- Realizar un diagnóstico de las necesidades específicas de capacitación en seguridad de la información.
- Construir material para sensibilización sobre seguridad de la información.
- Estructurar el Plan de Capacitación sobre seguridad de la información para el Banco Mundo Mujer.

2. CONTEXTUALIZACIÓN TEORICA

Este capítulo contiene los aspectos concernientes a la contextualización teórica la cual está integrada por un marco teórico, marco conceptual, marco legal y el marco situacional.

El marco teórico lo conforman las diversas teorías, estudios y demás conceptos referentes al desarrollo del problema planteado; el marco contextual tiene como función mostrar las condiciones y características más relevantes del contexto organizacional; el marco legal hace referencia a mencionar la base normativa bajo la cual se encuentra inmersa la organización objeto de estudio y específicamente las áreas involucradas; finalmente, el marco conceptual implica poner en contexto los diferentes términos y/o definiciones que se involucran en todo el desarrollo de la práctica profesional.

2.1 MARCO TEORICO

2.1.1 La Capacitación como término

El trabajo de práctica gira en torno a un Plan de Capacitación, y por ende la importancia de comprender el sentido amplio lo que el término capacitación representa a través de la historia. La capacitación ha existido desde hace tiempo, y representa un proceso de enseñanza - aprendizaje que busca modificar la conducta de una persona de forma planeada, según necesidades y con miras al logro de ciertos objetivos.

Según Grados Espinosa (2009) en su libro Capacitación y desarrollo del personal, “en la antigüedad (año 2001 a. C) la alfabetización se limitaba a ciertos sectores sociales y la única manera que había de comunicar los conocimientos era mediante la trasmisión verbal de generación en generación”; según este autor, los gremios fueron quienes constituyeron la primera forma de conceptos de empresa y dan origen a las agrupaciones de trabajadores, unidos por intereses comunes, un ejemplo de esto es la manera como trabaja Leonardo Da Vinci, entre los siglos XV y XVI, pues como maestro tenia aprendices a quienes les enseñaba sus oficios.

Los gremios conformados en la época, dieron paso a maestros artesanos quienes conformaban talleres exclusivos, demandando habilidad en la mano de obra, es así como la capacitación se

concibe inicialmente como una manera de conservar diferentes secretos de los oficios de la época[1], con el propósito de proteger intereses comunes de artesanos y comerciantes.

Con la Revolución industrial (1760-1840) a los trabajadores se les dejaba a cargo de un proceso productivo, para el cual se requería su destreza y conocimiento enfatizado, para Grados 2004 "Con la Revolución industrial, la capacitación se transformó con la incorporación de objetivos y métodos; por ejemplo, después de la aparición de los telares en Inglaterra, se pedía la participación de las personas para que pudieran trabajar en una sola actividad; es decir tenían a su cargo una parte del proceso de fabricación y lo realizaban". Es claro desde punto, que la industrialización provoco que los trabajadores se especializaran y se involucraran más en las actividades de producción.

Con el transcurrir del tiempo la industria creció irreversiblemente y la capacitación adquiere gran importancia, surgen entonces escuelas industriales[2] y diferentes instituciones encargadas del entrenamiento.

Dado lo anterior, surge la Calidad como modelo de gestión, impulsada inicialmente por los empresarios japoneses en la década de los 50 del siglo XX, donde el papel de los trabajadores en las organizaciones productivas, cambió radicalmente y la cultura organizacional comenzó a girar en torno a la eficiencia de los procesos, para lograr una mayor productividad, esto a su vez dio origen a una preocupación por parte de los empresarios en capacitar a los obreros, es así como hoy en día las capacitaciones hacen parte de estándares de calidad establecidos por normatividad y adoptados por casi todas las empresas.

Es así como a través de la historia la capacitación ha cobrado mayor importancia para el éxito de las organizaciones, y se convierte en un término usado frecuentemente, pero ¿Cómo se define puntualmente este término?, si bien la capacitación ha sido definida por muchos autores, cada uno de ellos tienen nociones diferentes y abordan el tema desde diferentes terminologías.

---

[1] Para Victoria Novelo (2003) en su libro: "La capacitación de artesanos en México", los jóvenes que se iniciaban barriendo, limpiando el taller o ayudando en cuestiones menores, paulatinamente iban aprendiendo los secretos del oficio, desde las etapas más sencillas, hasta finalmente conocían el proceso de producción perfectamente. (p. 54).

[2] "Con el crecimiento de la industria, la capacitación adquirió importancia, pues paso de la etapa en que solamente compartir un secreto dentro de un proceso, a la etapa de una sistematización de la enseñanza. En consecuencia surge la nueva forma de entrenamiento representada por las escuelas industriales, entre las que se encuentran HOE Y CIA (1872), WESTHINGHOUSE (1888), General Electric e International Harvester (1907). (Capacitación y desarrollo del personal, Grados Espinosa, 2009, p.207).

De acuerdo con la Real Academia Española (RAE), Capacitar es "formar, preparar, implica hacer a alguien apto, habilitarlo para algo". Por otro lado, Entrenar, "involucra la preparación a la práctica o adiestramiento a personas".

Según la consideración del autor Jaime A. Grados (2009)[3], el concepto de capacitación es "Acción destinada a incrementar las aptitudes y los conocimientos del trabajador con el propósito de prepararlo para desempeñar eficientemente una unidad de trabajo específico e impersonal".

Para Chiavenato (2007)[4] la capacitación "es el proceso educativo de corto plazo, aplicado de manera sistemática y organizada, por medio del cual las personas adquieren conocimiento, desarrollan habilidades y competencias en función de objetivos definidos".

En términos generales se define la capacitación como aquella acción, que involucra un proceso sistemático, que tiene como fin desarrollar habilidades y competencias en el personal de una organización, para hacer más eficiente el desarrollo de sus tareas y contribuir al logro de los objetivos organizacionales. Una organización que se preocupa por capacitar a sus colaboradores obtiene mejores resultados y reduce el riesgo de errores o eventualidades en sus procesos, sus empleados se sienten seguros en el manejo de sus actividades, saben tomar decisiones y son más eficientes.

2.1.3 Proceso de capacitación

Existen diferentes pasos o actividades en la estructuración de un plan de capacitación, en ese sentido según los autores William B. Werther y Keith Davis, en su libro Administración de Recursos Humanos (2008)[5], explican principalmente 4:

1. Evaluación de las necesidades: Según los autores la evaluación de las necesidades de capacitación, permite detectar problemas actuales y desafíos futuros que la organización debe enfrentar.

[3] Jaime A. Grados Espinosa (2009) Capacitación y desarrollo del personal, p.222

[4] Idalberto Chiavenato, (2007) Administración de Recurso Humanos, El capital humano de las organizaciones, p.386

[5] William B. Werther, Jr, Keith Davis (2008) Administración de Recursos Humanos, p.255

2. Objetivos de capacitación y desarrollo: Se constituyen como los resultados del paso 1, siendo necesario estipular los medios con los cuales se cuenta.

3. Contenido del programa: Su diseño debe ser acorde a las necesidades y los objetivos de capacitación planteados

4. Principios de aprendizaje: Los autores señalan que estos se define como los procesos por medio de los cuales las personas aprenden de manera efectiva y para ellos son la participación, repetición, relevancia, transferencia y realimentación.

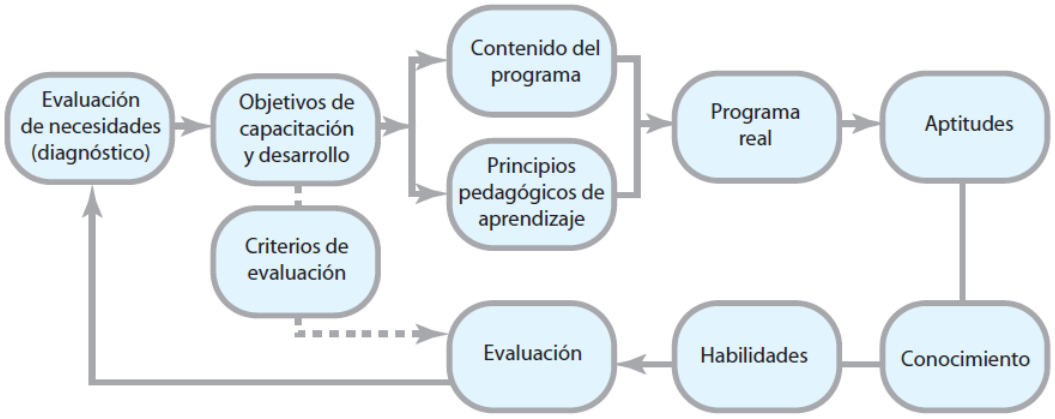


Figura 3. Pasos en la preparación de un Plan de capacitación y desarrollo
Fuente: Administración de Recursos Humanos, William B. Werther y Keith Davis (2008)

Para el autor Grados espinosa (2009)[6], el proceso de capacitación debe incluir 4 fases a implementar las cuales son:

A) Planeación.
B) Organización.
C) Ejecución.
D) Evaluación y seguimiento.

Dentro de estas fases se evidencias los pasos a seguir para la elaboración de un Plan de capacitación, Según Grados Espinosa, en la fase de Planeación, se determina que hacer y contiene 3 elementos: La detección de necesidades de capacitación (DNC), establecimiento de objetivos, y establecimiento de planes y programas; La fase de organización hace referencia al cómo hacerlo, se trata de definir los elementos humanos, tecnológicos, y físicos para su realización; La ejecución es la puesta en marcha del Plan, la realización y su puesta en marcha,

[6] Jaime A. Grados Espinosa (2009) Capacitación y desarrollo del personal, p.223.

implica los siguientes elementos: materiales y apoyos de instrucción, contratación de servicios y coordinación de cursos; finalmente la fase de evaluación y seguimiento, es la comprobación de lo alcanzado, respecto de lo planeado.

Por otra parte, según la Guía 14 del modelo de seguridad adoptado por El Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, para elaborar un adecuado Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información, se sugieren 4 fases (Figura 4) sucesivas, el diseño, la implementación, el desarrollo y el mejoramiento.

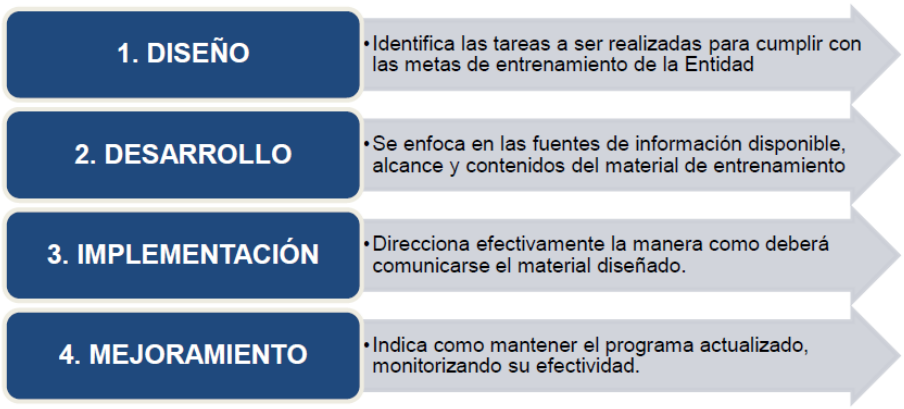


Figura 4. Fases plan de sensibilización y capacitación

Fuente: Guía 14, Plan de Capacitación y Sensibilización De Seguridad De La Información, MINTIC.

Considerando el enfoque cualitativo de la investigación, la información primaria y los diferentes pasos descritos para la elaboración de un Plan de Capacitación, el Plan de Capacitación y Sensibilización en Seguridad de La información para el Banco Mundo Mujer seguirá un proceso y metodología, que permita el logro de los objetivos propuestos en la presente práctica profesional, y es la siguiente:

1. Identificación de las necesidades: Esta identificación de las necesidades de capacitación se realizaran a través de un diagnóstico, el cual tendrá como insumos información proveniente principalmente de la matriz de riesgos en seguridad de la información y una investigación cualitativa desde mi rol como practícate de las necesidades de capacitación en SI. A partir de este diagnóstico se empieza a estructurar el Plan de capacitación y sensibilización en Seguridad de la información.

2. Objetivos de capacitación y desarrollo: En este paso se establecerán todos los objetivos de la capacitación, los cuales deben ser coherentes con las necesidades, los recursos y los medios disponibles para su consecución.

3. Contenido del Plan o Programa: Se diseñara el Contenido del Plan de acuerdo a la evaluación de necesidades y los objetivos de aprendizaje, teniendo en cuenta no solo las necesidades del Talento Humano sino también las del área y la organización en general. Se plantearan estrategias que permitan el éxito del plan, así como herramientas y material didáctico, que sensibilice y promueva el aprendizaje.

4. Evaluación del Plan de capacitación: La evaluación se hace como resultado de la implementación del plan, la cual no se realizara durante la práctica profesional, por ende en este paso solo se describirán los criterios de evaluación y se proporcionaran materiales que permitan esta evaluación.

2.1.4 Herramientas de diagnostico

Para realizar un adecuado Diagnostico de las Necesidades de Capacitación (DNC) es necesario identificar bien el problema, no es suficiente con la apreciación de una sola persona, para esta identificación se utilizara como herramienta el árbol de problemas, siendo este el más adecuado por ser un análisis basado en una lluvia de ideas.

Según el manual 39 del Instituto Latinoamericano y del Caribe de Planificación Económica y Social (ILPES)[7] Área de proyectos y programación de inversiones, los pasos a seguir que se sugieren son los siguientes:

1. Analizar e identificar lo que se considere como problemas principales de la situación analizada, debido a que surgen múltiples causas que pueden explicar el problema y los efectos que se derivan de ello.
En términos de análisis se recomienda que a partir de una primera “lluvia de ideas” establecer cuál es, a juicio del grupo de analistas, el problema central, aplicando criterios de prioridad y selectividad.

[7] Edgar Ortegón, Juan Francisco Pacheco y Horacio Roura (2005), *Metodología general de identificación, preparación y evaluación de proyectos de inversión pública*, (ILPES) Área de proyectos y programación de inversiones, Santiago de Chile.

2. Definir los efectos más importantes del problema, de esta forma se analiza y verificar su importancia.
3. Anotar las causas del problema central detectado, lo que significa buscar qué elementos están o podrían estar provocando el problema.
6. Una vez que tanto el problema central, las causas y los efectos están identificados se construyen los "Diagramas del árbol de efectos y causas" asociados al problema.

Para el primer paso, la identificación del problema la guía sugiere que el problema central se debe formular en forma negativa, haciendo claridad en que este no representa la ausencia de algo, no es una carencia o déficit y debe referirse a una situación real no ficticia sobre la población objeto de estudio definida; desde una perspectiva similar, según Kerlinger[8] (1975), los criterios para plantear adecuadamente el problema de investigación son:

1. El problema debe expresar una relación entre dos o más variables.
2. El problema debe estar formulado claramente y sin ambigüedad como pregunta
3. El planteamiento debe implicar la posibilidad de realizar una prueba empírica. Es decir, de poder observarse en la realidad

En el segundo paso se definen los efectos del problema, los cuales una vez se identifique el problema principal, se grafican hacia arriba, teniendo en cuenta que hay efectos que dan a origen a otros, generando reacción en cadena lo que se denomina según ILPES (2005) "encadenamiento de los efectos", como se ilustra en la Figura 5. *Árbol de efectos*.

En el tercer paso siguiendo la anterior metodología, se identifican las causas del problema y se sugiere que su secuencia se inicie con las más relacionadas al problema central.

Finalmente como cuarto punto, la guía sugiere la gráfica completa del árbol de problemas como se ilustra en la Figura 6, esta grafica es el resumen detallado del problema analizado, y representa el punto inicial del DNC, con base en este primer análisis se inicia la detección de las necesidades de capacitación en seguridad de la información, las cuales se establecen con la reunión de los expertos y se delimitan con el uso de la técnica del Abaco de Regnier.

[8] Hernández Sampieri, Roberto. (2006). "Planteamiento del problema: objetivos, preguntas y justificación del estudio" en Metodología de la Investigación. México, p. 10.

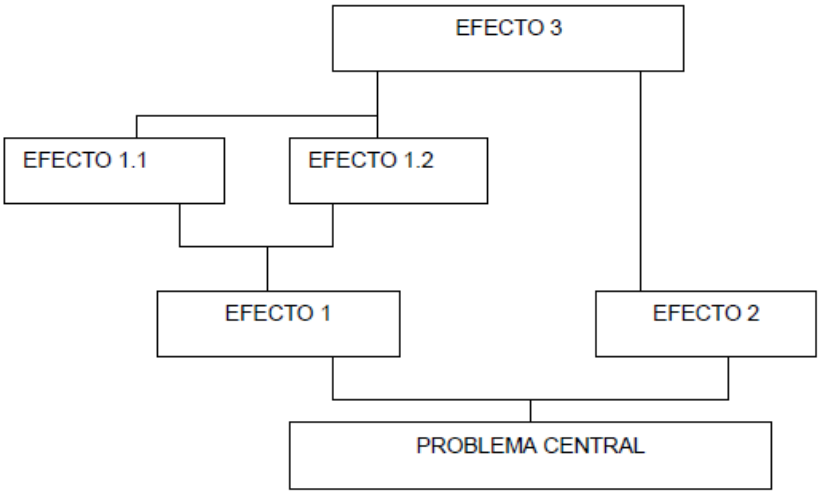


Figura 5. Árbol de efectos
Fuente: ILPES, Área de proyectos y programación de inversiones

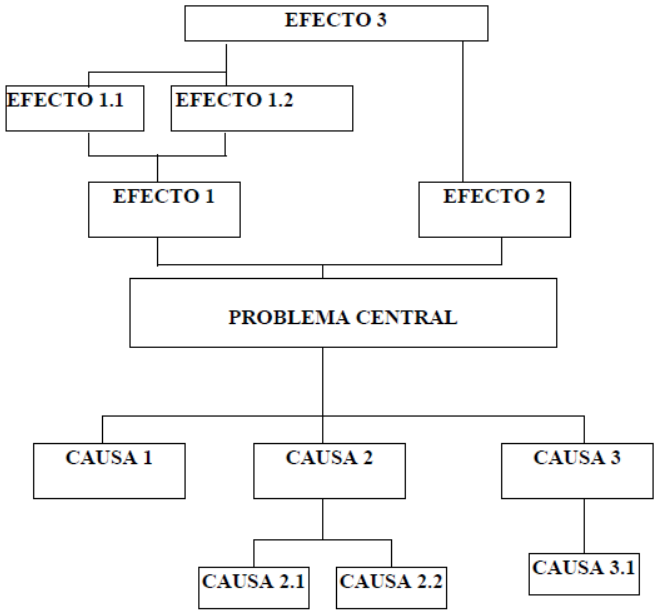


Figura 6. Árbol de Problemas
Fuente: ILPES, Área de proyectos y programación de inversiones

Esta herramienta fue planteada por el Doctor François Régnier, con el fin de interrogar a expertos y tratar sus respuestas a partir de una escala de colores, esta herramienta permitirá definir el contenido del programa de capacitación y sensibilización, según Sastoque (1991) “la importancia del Abaco radica en que nos permite medir las actitudes de un grupo frente a un

tena determinado" (p. 21), en este caso la actitud del grupo de expertos frente a las diferentes necesidades de capacitación.

Para entender mejor esta metodología, la actitud del grupo de expertos frente al tema tratado, se asemeja a los colores del semáforo, donde el verde es un color favorable (siga), el amarillo un color Intermedio (prepárese) y el rojo un color desfavorable (pare), la actitud u opinión de cada experto se delimita las siguientes opciones:

OPINIÓN	COLOR	SIGNIFICADO
R		No incide
r		Incide muy poco
A		Neutro
v		Incide algo
V		Incide Mucho
B		Participa sin opinión
N		No participa

Figura 7. Opciones del Abaco de Regnier

Como **primer paso**, cada experto da su opinión del tema en un formulario individual, según las opciones anteriormente descritas, como se ilustra en la Figura 8.

Una vez se obtiene la opinión de todos los expertos frente al tema abordado, se continua con el **segundo paso**, en el que se analizan los datos y se organiza cada ítem (necesidad de capacitación) frente a la opinión de cada experto, con el color correspondiente, es importante resaltar que esta información hace visible simultáneamente la posición de cada uno de los expertos sobre los ítems, como se ilustra en la Figura 9, por ende se recomienda que cada experto justifique su decisión de voto.

En el tercer paso, se realiza el procesamiento de los datos, que según Sastoque (1991) pueden clasificarse inicialmente en filas o columnas, en filas se organizarían los ítems y se lograría apreciar su importancia, como se ilustra en Figura 10, y en columnas se conocería la opinión de cada experto y se podría clasificar según los votos, como se muestra en la Figura 11.

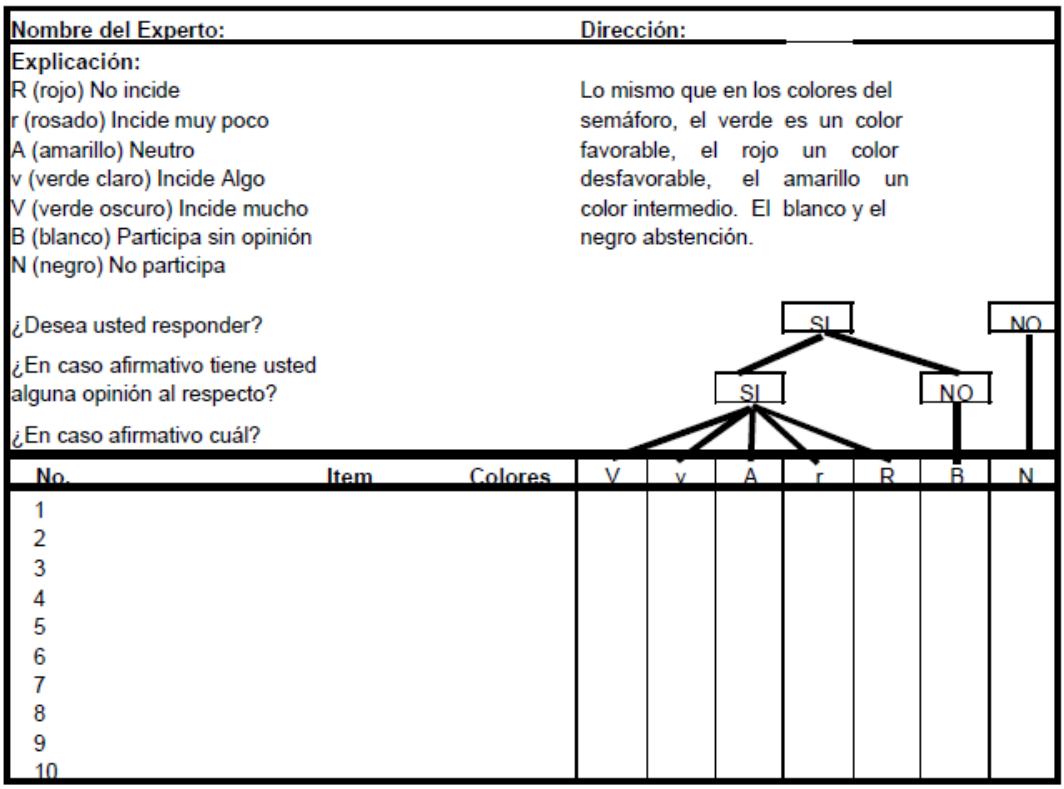
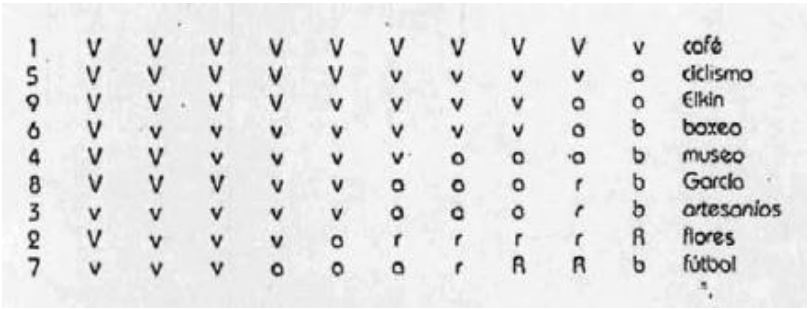


Figura 8. Cuestionario Abaco de Regnier
Fuente: M. Sastoque, Francisco, El Abaco de Regnier. En La Prospectiva (21-33). Bogotá: Legis Editores (1991)

ITEM	EXPERTOS								
	A	B	C	D	E	F	G	H	I
1	V								
2	R								
3	v								
4	r								
5									
6									
7									
8									
9									
10									

Figura 9. Abaco de Régnier, Análisis De Datos
Fuente: Sastoque, Francisco, El Abaco de Regnier (1991)



1	V	V	V	V	V	V	V	V	V	v	café
5	V	V	V	V	V	v	v	v	v	o	ciclismo
9	V	V	V	V	v	v	v	v	o	o	Elkin
6	V	v	v	v	v	v	v	v	o	b	boxeo
4	V	V	v	v	v	v	o	o	o	b	museo
8	V	V	V	v	v	o	o	o	r	b	García
3	v	v	v	v	v	o	o	o	r	b	artesanías
2	V	v	v	v	o	r	r	r	r	R	flores
7	v	v	v	o	o	o	r	R	R	b	fútbol

Figura 10. Abaco de Régnier, Clasificación por filas
Fuente: Sastoque, Francisco, El Abaco de Regnier (1991) p.30

	H	I	F	D	G	J	B	C	A	E	
1	V	V	V	V	V	V	V	v	V	V	Café
5	v	V	V	V	V	V	o	v	v	v	Ciclismo
6	v	v	V	v	v	v	v	b	o	v	Boxeo
4	V	V	v	v	v	o	v	b	o	o	Museo
9	V	v	V	V	o	R	v	v	v	o	Elkin
3	v	v	o	r	v	v	v	b	o	o	Artesanías
8	V	V	r	r	o	V	v	b	o	r	García
2	V	r	r	v	o	r	R	v	v	r	Flores
7	o	r	v	o	o	v	b	R	R	v	Fútbol

Figura 11. Abaco de Régnier, Clasificación por Columnas
Fuente: Sastoque, Francisco, El Abaco de Regnier (1991) p.31

Finalmente se obtienen los ítems que más inciden (Verde Oscuro), hasta los que se consideran No inciden (Rojo), y se conoce también la opinión de los expertos frente a cada uno de ellos. Esta herramienta es fundamental al momento de determinar las necesidades de capacitación, ya que se delimita de manera práctica el alcance del Plan y se toma en cuenta todos los puntos de vista los expertos.

2.2 MARCO CONTEXTUAL

El marco situacional comprende la caracterización de la organización objeto de estudio en la cual se desarrollara la práctica profesional, en este caso: Banco Mundo Mujer.

Este acápite comprende 4 partes. En primer lugar se describe el contexto de la organización objeto de estudio; en segundo lugar se encuentra el direccionamiento estratégico; en tener lugar se describen los productos y servicios del BMM y finalmente se realiza una descripción detallada del área específica en la cual se desarrolló la práctica profesional.

2.2.1 Historia de la organización

El Banco Mundo Mujer cuenta con 167 oficinas y 64 corresponsales en el territorio Colombiano.

Tabla 1. Información del Banco Mundo Mujer

ITEM	BANCO MUNDO MUJER SA
NIT	900768933-8
Dirección Principal	Carrera 11 # 5-56 Barrio Valencia
Ciudad y Departamento	Popayán – Cauca
Teléfono	8 39 99 00
Aseguradora de RL	Positiva Compañía de Seguros
Clase de Riesgo Laboral	Clase de Riesgo 1
Código de la Actividad Económica. 1.651201	Actividades de los bancos diferentes del banco central hace referencia a empresas dedicadas a la recepción de depósitos a la vista, en cuenta corriente bancaria, trasferencias por cheque, captación de otros depósitos a la vista o a término, con el objetivo de realizar operaciones activas de crédito (bancos, seguros, instituciones de finanzas y/o crédito en general. Decreto 1607/02.
Clasificación de Actividades económicas según CIIU. 6412	Las actividades de entidades que tienen como función principal la captación de recursos en cuenta corriente bancaria, así como también la captación de otros depósitos a la vista o a término (cuentas de ahorro, certificados de depósito a término [CDT], entre otros). Transferibles por cheque o medio electrónico con el objeto de realizar operaciones activas de crédito. Cámara de Comercio.

Fuente: Banco Mundo Mujer

En Popayán, capital del departamento del Cauca y con la filosofía del Banco Mundial de la Mujer, nació en el año 1985 la Fundación Mundo Mujer como una Organización No

Gubernamental, ONG, que con el paso de los años se convirtió en la entidad de microcrédito con mayor desarrollo económico y beneficio social de esta región y del país.

Con la experiencia de 29 años en el mercado atendiendo a las comunidades estrato uno, dos y tres de Colombia, otorgando microcrédito de una manera fácil, rápida y oportuna y con atención personalizada, permitiendo la inclusión financiera, promoviendo el empoderamiento, autoestima e independencia de la mujer y en aras de ofrecer nuevos productos a la comunidad; la Fundación Mundo Mujer decide iniciar su proceso de evolución a banco.

Es así como el 18 de diciembre del 2014 la entidad recibe con gran satisfacción la autorización de la Superintendencia Financiera de Colombia para operar como un banco y desde febrero de 2015 abre sus puertas, MUNDO MUJER EL BANCO DE LA COMUNIDAD.

2.2.2 Direccionamiento estratégico

Desde su constitución como Banco (2015), se estableció el siguiente direccionamiento:

MISIÓN

Contribuimos al desarrollo económico de las comunidades trabajadoras del país, estimulando el ahorro y generando acceso fácil y oportuno al crédito y a los servicios financieros complementarios, mediante una metodología personalizada, que genera crecimiento y desarrollo del talento humano de la organización, rentabilidad para los accionistas y la entidad, garantizando su solidez y permanencia en el tiempo.

VISIÓN

Seremos el Banco Líder de la Comunidad.

VALORES

- Humildad: Aceptarnos como somos y reconocer nuestras debilidades para mejorar.
- Integridad: Actuar con honestidad para generar confianza.
- Liderazgo: Responsabilidad que entraña conducir personas y cumplir objetivos.
- Excelencia: Constancia, responsabilidad, efectividad.
- Respeto: Para influir, generar afiliación y ser admirado.

2.2.3 Productos y servicios del Banco Mundo Mujer

El Banco Mundo Mujer cuenta con los siguientes productos y servicios financieros:

1. **Crédito para negocio**: Financian tiendas, ventas por catálogo, ventas de comida, ventas de ropa y cualquier tipo de negocios, desde $800.000 hasta $41.000.000, si usted es cliente de hasta $93.749.040.
2. Crédi**to agropecuario:** Financiamiento de cultivos, cría de animales y toda actividad relacionada con el sector agropecuario, desde $800.000 hasta $11.000.000, para los clientes hasta $21.000.000.
3. **Crédito para pequeña empresa:** Financiamiento de Pequeñas Empresas que desarrollen actividades de negocio, comercio o producción, desde $800.000 hasta $109.373.880, si es cliente hasta $234.372.600.
4. **Crédito de libre inversión:** Financiamiento de viajes, estudio, electrodomésticos, muebles y artículos de valor, desde $800.000 hasta $11.000.000, y de $21.000.000, para los clientes.
5. **Cuenta de ahorro gratis:** Pago de intereses, sin cobro de cuota de administración, una persona natural puede abrir su cuenta desde $50.000 y una persona jurídica desde $100.000.
6. **Cuenta de ahorro con tarjeta de crédito**
7. **Cuenta de ahorro Chikiteens:** Cuenta de ahorro a nombre del niño, con beneficios de tasa de interés, y estrategias de aprendizaje como el tarjetón de juegos, y obsequios al abrir la cuenta.
8. **Cuenta tu meta:** Se programa un plan de ahorro y se gana intereses al cumplirlo.
9. **CDT progrese**
10. **Seguro de deuda:** Un seguro es un contrato por el cual una aseguradora se compromete a compensar económicamente, al tomador del seguro o a sus beneficiarios, cuando ocurra un evento inesperado.
11. **Seguro familia protegida:** Son 4 planes con diferentes montos del seguro y beneficios.

2.2.4 Área del desarrollo de la práctica

El área de Seguridad de la Información en la cual se desarrolla la práctica profesional, hace parte de la vicepresidencia de riesgos la cual está estructurada de la siguiente manera:

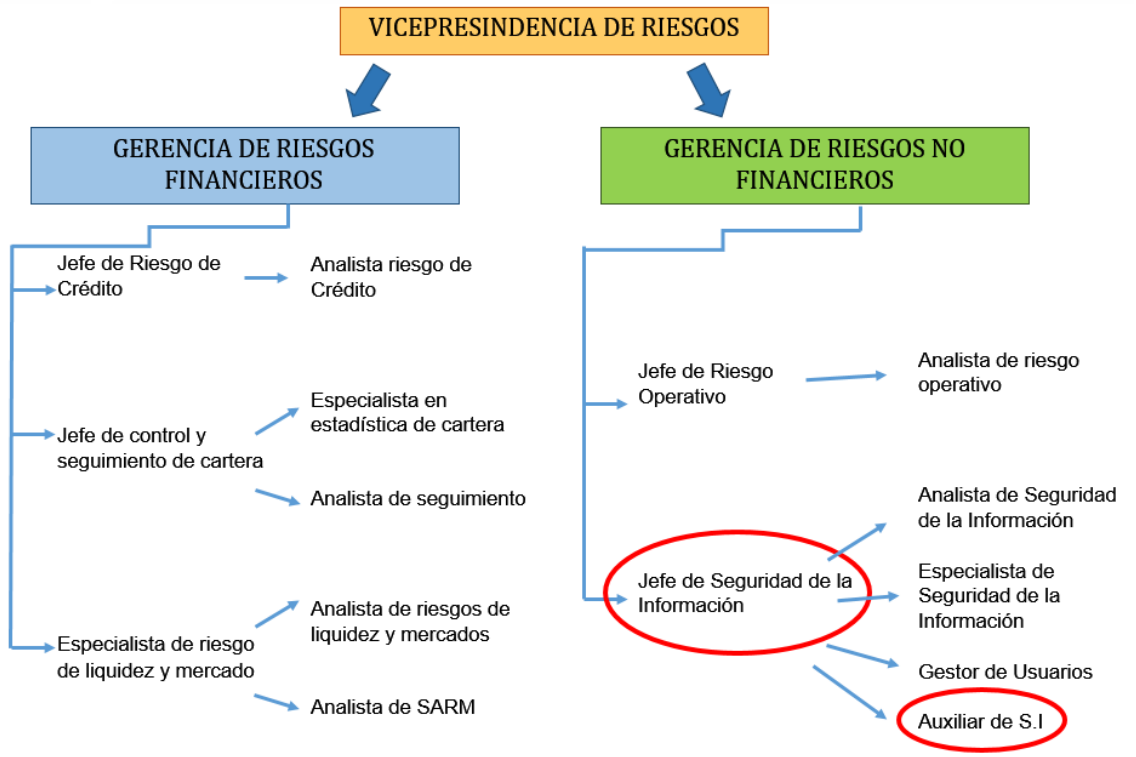


Figura 12. Jerarquización área de riesgos

RIESGOS FINANCIEROS Y NO FINANCIEROS

Es necesario abordar brevemente la temática de riesgos, para contextualizar mejor los diferentes aspectos de naturaleza interna de la organización, relacionados con el área en la cual se desarrolla la práctica profesional

El evidente crecimiento de la economía y del mercado financiero lo hace más dinámico y propenso a diferentes vulnerabilidades, obligando a las instituciones financieras a gestionar cada vez mejor el riesgo, entendido como "la posibilidad de sufrir un daño" (Banco Interamericano de Desarrollo, 1999, p.4)

Considerando lo anterior el Banco Mundo Mujer asume una serie de riesgos, los cuales debe gestionar eficientemente, convirtiendo a la vicepresidencia de Riesgos en una de las más importantes dentro de la estructura general, ya que desde allí se gestionan todos los riesgos relacionados con las operaciones del banco.

La vicepresidencia de riesgos se divide en dos gerencias, la gerencia de riesgos financieros y la gerencia de riesgos no financieros, la primera hace referencia a al riesgo financiero que según los autores Diego Gómez y Jesús López Zaballos (2002), se define como: "la posibilidad de quebranto o pérdida derivada de la realización de operaciones financieras que pueden afectar a la capitalización bursátil o valor de mercado de la empresa" (p. 21), es decir la posibilidad de ocurrencia de un evento que tenga consecuencias financieras negativas para una organización; la gerencia de riegos financieros se compone de:

1. Riesgo de Crédito: Posible pérdida que asume el Banco, por incumplimiento de las obligaciones de los clientes.

2. Riesgo de liquidez y mercado: El riesgo de liquidez se refiere a la posible pérdida que se asume por no disponer de recursos líquidos suficientes para cumplir con las obligaciones, y el riesgo de mercado a posibles pérdidas derivadas de la dinámica del mercado.

Por otra parte los riesgos no financieros, hacen referencia a riesgos derivados de los procesos de la organización, y se dividen en riesgo operativo y Seguridad de la Información.

1. Riesgo Operativo: Esta área se encarga de levantar y actualizar constantemente las matrices de riesgo de los diferentes procesos de cada área del banco.

2. Seguridad de la información: Es la responsable de garantizar la confiabilidad, integridad y disponibilidad de la información.

Ahora bien, los diferentes riesgos del Banco Mundo Mujer se identifican y controlan desde el área de riesgo Operativo, con base en el levantamiento de una matriz de Riesgo Operativo para cada área, en términos generales en esta matriz se identifican los riegos de los procesos, sus causa/s, se describen los controles y se establecen los planes de acción para mitigar estos riesgos.

IDENTIFICACIÓN DE LOS PROCESOS

Para la elaboración del Plan de Capacitación y sensibilización, es importante conocer los procesos del área de seguridad de la información, ya que estos proporcionan una visión más amplia sobre el enfoque que debe tener el Plan (contenido del programa, objetivos de capacitación,), estos procesos son los siguientes:

1. PR 017: Administración de Usuarios y Perfiles, administrar la adecuada asignación de usuarios y perfiles según los cargos establecidos.
2. PR 014: Intercambio de información con terceros
3. PR 034: Gestión de Usuarios sensitivos (Usuarios sin restricciones de acceso a los sistemas de información)
4. PR 056: Administración de activos de hardware y software
5. PR 081: Aseguramiento de infraestructura Tecnológica.
6. PR 086: Gestión de Vulnerabilidades.
7. PR 007: Seguridad de la información (Listas Blancas).
8. PR105: Administración y Control de Pasos entre ambientes.
9. PR 033: Backup y restauración de datos.

Para definir las necesidades y el contenido programático del Plan de capacitación y sensibilización, es necesario conocer también las políticas generales establecidas en materia de seguridad de la información, ya que estas son la principal guía para el desarrollo de las actividades diarias de todos los colaboradores del Banco. Entre estas se encuentran las siguientes:

1. Uso de Contraseñas
2. Escritorio Limpio
3. Uso del servicio de internet
4. Control de puertos USB.
5. Uso y control de portátiles
6. Escritorio y Pantalla Limpia
7. Uso del servidor de archivos
8. Intercambio de archivo con terceros
9. Clasificación de la información
10. Destrucción de la información
11. Uso de WhatsApp corporativo
12. Áreas seguras
13. Equipos de comunicación de red.
14. Requisitos de Seguridad de los sistemas de información.
15. Uso de controles criptográficos

2.3 MARCO LEGAL

El desarrollo de la práctica profesional, involucra la mención de normatividad legal inmersa en el trabajo, siendo necesaria su mención como referencia orientadora; además, el Banco Mundo Mujer de la ciudad de Popayán, como organización se rige bajo determinada normatividad legal, la cual se debe tener en cuenta.

Tabla 2. Marco Legal del Plan de Capacitación y Sensibilización en SI

NORMATIVA	DESCRPCIÓN
Constitución Política de Colombia 1991 Art 335.	Incluye diferentes generalidades.
Ley 663 de 1993	Estatuto Orgánico Financiero.
Ley 526 de 1999	Por medio de la cual se crea la Unidad de Información y Análisis Financiero (UIAF)
Ley 599 de 2000	Código Penal Colombiano.
Ley 1712 de 2014	Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.
Decreto 1727 de 2009	Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información" .
ISO 27001:2013	**Sistemas de gestión de seguridad de la información:** Modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI).
ISO 31000	**Gestión del riesgo:** Establece un número de principios necesarios a establecer para hacer eficaz la gestión del riesgo en las organizaciones.

LEY 1273 DEL 2009	**De la protección de la información y de los datos** "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".
Ley 1266 de 2008. “	Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.
Ley 1314 de 2009	Regula los principios y normas de contabilidad e información financiera y de aseguramiento de información aceptados en Colombia, señala las autoridades competentes, el procedimiento para su expedición y se determinan las entidades responsables de vigilar su cumplimiento.
Ley 1266 de 2008	Dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1581 de 2012	**Protección de datos personales:** Se dictan disposiciones generales para la protección de datos personales.

2.4 MARCO COCEPTUAL

Para lograr una comprensión precisa del trabajo de práctica a desarrollar, es importante dominar de forma inequívoca diversos términos involucrados, que además permitirán sistematizar de forma correcta la realidad.

BMM: Siglas del Banco Mundo Mujer.

CIS: Área de Centro Integral de Servicios del Banco Mundo Mujer.

S.I: Siglas de Seguridad de la Información.

Área de Tecnología de la Información: Área encargada de soportar, diseñar y mantener activos electrónicos y el hardware del banco

Sistema de Gestión de Seguridad de la Información (SGSI). Se basa en un enfoque de riesgo de negocios, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información, que incluye estructura, políticas, actividades de planeación, responsabilidades, prácticas, procedimientos, procesos y recursos de la Entidad.

Activo: Cualquier cosa que tenga valor para la organización.

Activos de información. Es todo activo que contenga información, la cual posee un valor y es necesaria para realizar los procesos del negocio y de soporte de EL BANCO. Se pueden clasificar en: Personas, Intangibles, Electrónicos, físicos y Servicios.

Información sensible. Es una categoría especial de datos de carácter personal especialmente protegido, que hacen parte del haber íntimo de la persona y pueden ser recolectados únicamente con el consentimiento expreso e informado de su titular y en los casos previstos en la ley: Salud, Sexo, Filiación política, Raza u origen étnico.

Capacitación: Acción, que involucra un proceso sistemático, que tiene como fin desarrollar habilidades y competencias en el personal de una organización, para hacer más eficiente sus tareas y contribuir al logro de los objetivos organizacionales.

Sensibilización: es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.

Entrenamiento: Proceso utilizado para enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas su cargo.

SGSI: Hace referencia al Sistema de Gestión de Seguridad de la Información, elaborado por el área de Seguridad de la información, el cual incluye varios elementos, como políticas, procedimientos , entre otros.

Software malicioso: es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

Backup: Copia de respaldo almacenada en el servidor a un dispositivo de almacenamiento externo.

Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Disponibilidad: es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Integridad: es la protección de la exactitud y estado completo de los activos.

Perfil: Nivel de acceso a determinada información como la consulta, modificación y administración.

Privilegios: Permiso de acceso a una plataforma o sistema de información.

Riesgo inherente: Es el riesgo intrínseco de cada actividad, sin tener en cuenta los controles que de éste se hagan a su interior

Riesgo residual: Es aquel riesgo que subsiste, después de haber implementado controles.

3. CONTEXTUALIZACIÓN METODOLOGICA

Este capítulo está compuesto por las estrategia metodológicas utilizadas durante el desarrollo de la práctica, en él se describe la tendencia investigativa, la metodología, las fuentes de información y los instrumentos de análisis a utilizar para el logro de los objetivos propuestos.

3.1 Diseño de la Investigación

"El termino diseño hace referencia al plan o estrategia concebida para obtener la información que se desee, en ese sentido existen dos grandes enfoques, la investigación de tipo cuantitativa y la investigación de tipo cualitativa (…)" (Marcelo M. Gómez, Introducción a la metodología de la investigación Científica, pág. 85,2006)

La investigación que se llevara a cabo en el desarrollo de la práctica, es de tipo cualitativo; se debe agregar que según Pita Fernández y Pértegas Díaz (2002), La investigación cuantitativa es aquella en la que se recogen y analizan datos cuantitativos sobre variables mientras que la investigación cualitativa evita la cuantificación; Taylor y Bogdan (1986) opinan que la investigación cualitativa es aquella que:

"…produce datos descriptivos: las propias palabras de las personas, habladas o escritas, y la conducta observable".

En ese sentido la investigación cualitativa es la más acertada para alcanzar los objetivos propuestos, ya que permite identificar los procesos claves del área de seguridad de la información su análisis y posterior diagnóstico de las necesidades de capacitación.

3.2 Metodología de la Investigación

La principal metodología de la investigación que se utilizara será la etnografía[9], y el instrumento mediante el cual se recogerá la información es la investigación participativa[10], siendo esta una

[9] Hace referencia al estudio directo de personas y grupos durante un cierto periodo, utilizando la observación participante o las entrevistas para conocer su comportamiento social (Giddens, 1994)

[10] Según Taylor y Bogdan (l986) esta "involucra la interacción social entre el investigador y los informantes en el medio de los últimos, y durante la cual se recogen los datos de modo natural y no intrusivo".

de las técnicas más utilizadas en la investigación cualitativa, puesto que permite extraer gran cantidad de datos para desarrollar la práctica, al estar directamente involucrado en el problema o la situación a analizar.

Además se utilizaran otras técnicas como las entrevistas abiertas no estructuradas, la revisión de documentos, la evaluación de experiencias personales y la discusión grupal con los analistas del área de seguridad.

3.3 Fuentes de Información

En cuanto a las fuentes de recolección de datos, de las cuales se obtiene la información necesaria para el desarrollo del plan estratégico, se puede hablar de dos: La primera fuente de información son los datos primarios o directos y la segunda fuente son los datos secundarios; como datos primarios se encuentra la información suministrada por directamente por el banco, como las políticas de seguridad de la información y los principales riesgos en seguridad de la información detectados por el área de Riesgo Operativo; los datos secundarios están constituidos por aquellos documentos y/o información que sirven de referencia para la elaboración del presente plan, como investigaciones, artículos y referencias bibliográficas.

3.4 Instrumentos de Análisis

Como se definió anteriormente, el instrumento de análisis a utilizar es la investigación participativa u observación participante y la forma en cómo se obtendrán los datos es la siguiente:

Tabla 3. Instrumentos de Análisis

INSTRUMENTO DE ANALISIS	DESCRIPCIÓN
Entrevistas abiertas	Esta técnica consistirá en realizar una serie de entrevistas no estructuradas con los analistas del área de seguridad y los analistas de riesgo operativo, para obtener información relevante respecto a los principales riesgos en seguridad de la información,

	determinar las necesidades de capacitación y sensibilización.
Información secundaria	Se revisaran las diferentes matrices de riesgo operativo del área de seguridad, para conocer los riesgos en seguridad de la información; además, se analizaran las políticas establecidas en el SGSI, como principal material para definir las temáticas de capacitación y sensibilización.
Observación directa	Las vivencias diarias proporcionan información valiosa, sobre el contenido temático del plan de capacitación en temas de seguridad de la información.

4. DESARROLLO DEL TRABAJO DE PRÁCTICA PROFESIONAL

PLAN DE CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN PARA EL BANCO MUNDO MUJER DE LA CIUDAD DE POPAYÁN PARA PRIMER SEMESTRE DE 2018.

INTRODUCCIÓN

Actualmente las organizaciones no pueden garantizar la confidencialidad, disponibilidad e integridad de la información sin la participación de las personas que utilizan los recursos informáticos, activos de información y la información en sí misma. El mecanismo que permite involucrar al recurso humano en este proceso es la educación y el entrenamiento en seguridad de la información, mediante el cual, todos los empleados de la organización pueden llegar a conocer sus responsabilidades, riesgos de seguridad, y acciones a seguir en caso de presentarse un incidente de seguridad, que pudiera poner en peligro la operación continua de la función misional.

Ahora bien, teniendo como antecedentes los constantes ataques y amenazas relacionados con el robo de información confidencial en el sector financiero a nivel mundial, el Banco Mundo Mujer ha establecido un Sistema General de Seguridad de la Información, con el objetivo de brindar los lineamientos necesarios para asegurar un adecuado manejo de la información de las diferentes operaciones del banco.

Para ello, el Plan de Capacitación y Sensibilización en Seguridad de la Información, es un instrumento de mejora, sustentado en un marco teórico y que responde a una problemática presente en el Banco Mundo Mujer, este a su vez se compone de un conjunto de acciones formativas encaminadas a fortalecer los conocimientos y mejorar las prácticas diarias de los colaboradores del banco

Dicho plan, se conforma de 4 parte a saber: En primer lugar, se identificaron las necesidades de capacitación tomando como referencia la matriz de riesgos y la información de los analistas (enfoque cualitativo); en segundo lugar se definieron los objetivos de capacitación; en tercer lugar se estableció el contenido del plan o programa, y se determinaron las estrategias para lograr implementación.

Finalmente se elaboró un banco de preguntas como forma de evaluación para las jordanas de capacitación.

ANTECEDENTES

El Banco Mundo Mujer a lo largo de su trayectoria, ha establecido y ejecutado periódicamente diferentes planes y acciones de formación y capacitación, dirigidas principalmente a nuevos colaboradores de diferentes cargos, tales como directivos, personal administrativo y de apoyo, con el fin de dar a conocer las diferentes áreas, procesos y políticas establecidas dentro de la organización.

Cabe mencionar, que la periodicidad de estas capacitaciones depende del flujo de ingreso de nuevo personal, de esta manera se puede asegurar que todos y cada uno de los colaboradores de la dirección general del Banco han sido capacitados de manera presencial y en línea.

Existen varios planes de capacitación establecidos por las diferentes áreas que conforman el Banco, como por ejemplo el Plan de Capacitación en Seguridad y Salud en el trabajo, liderado desde el área de Talento Humano; Cabe resaltar que los hasta aquí mencionados planes, son de carácter general, es decir que están dirigidos a todos los colaboradores de la dirección General del Banco.

Desde el año 2015, momento en el cual la Fundación Mundo Mujer en la ciudad de Popayán se constituye y opera formalmente como entidad Bancaria, denominándose Banco Mundo Mujer, empieza una reestructuración, que incluye la preocupación constante por contar con personal profesional y capacitado en todas las áreas

Ahora bien, específicamente en temas de seguridad de la información, el Banco dentro de su capacitación a nuevo personal, incluye las áreas más relevantes, como son: **Sarlaft, Control Interno, Continuidad del Negocio, Talento Humano, Mercadeo, Riesgo Operativo, y seguridad de la información,** entre otras; Cada colaborador del banco sin importar el área, realiza una evaluación y recibe certificación virtual

1. DIAGNOSTICO DE LAS NECESIDADES DE CAPACITACIÓN

1 1. IDENTIFICACIÓN DEL PROBLEMA

Es importante definir puntualmente las causas por las cuales gran parte de los colaboradores del Banco tienen bajo nivel de formación en temáticas de seguridad de la información, para esto se utilizara como herramienta el árbol de problemas, cuyo objetivo es identificar las causas y efectos reales de un problema central. Su construcción se realizó con base en la opinión de los siguientes expertos, a saber:

Tabla 4. Panel de Expertos

NOMBRE	CARGO
Víctor Daniel Mosquera	Vicepresidente de Riesgos
Juan Pablo Rodríguez	Jefe de Riesgos no financieros
Andrea Linares	Jefe de Riesgo Operativo
Julieth Guevara	Analista de Seguridad de la Información
Marcela Solano	Analista de Seguridad de la Información
Carlos Rodallega	Especialista de Seguridad de la Información

Con la participación de este grupo de trabajo, se logra estructurar el árbol de problemas de la Figura 13, que permite sintetizar de manera objetiva la problemática abordada.

1.2 DETECCIÓN DE LAS NECESIDADES DE CAPACITACIÓN

El diagnóstico de las necesidades de capacitación se ha efectuado utilizando técnicas de recolección de información, las cuales se describen a continuación:

- ✓ **Información Secundaria:** Documentos formales del área de Seguridad.
- ✓ **Entrevistas abiertas:** Entrevistas no estructuradas con los analistas del área de seguridad y los analistas de riesgo operativo. Las entrevistas
- ✓ incluyen tres niveles de participación, representados por los analistas del área de S.I, Riesgo Operativo, y el gerente de riesgos no financieros.

- ✓ **Observación.** Instrumento de investigación cualitativa, que permite realizar un análisis directo del entorno laboral.

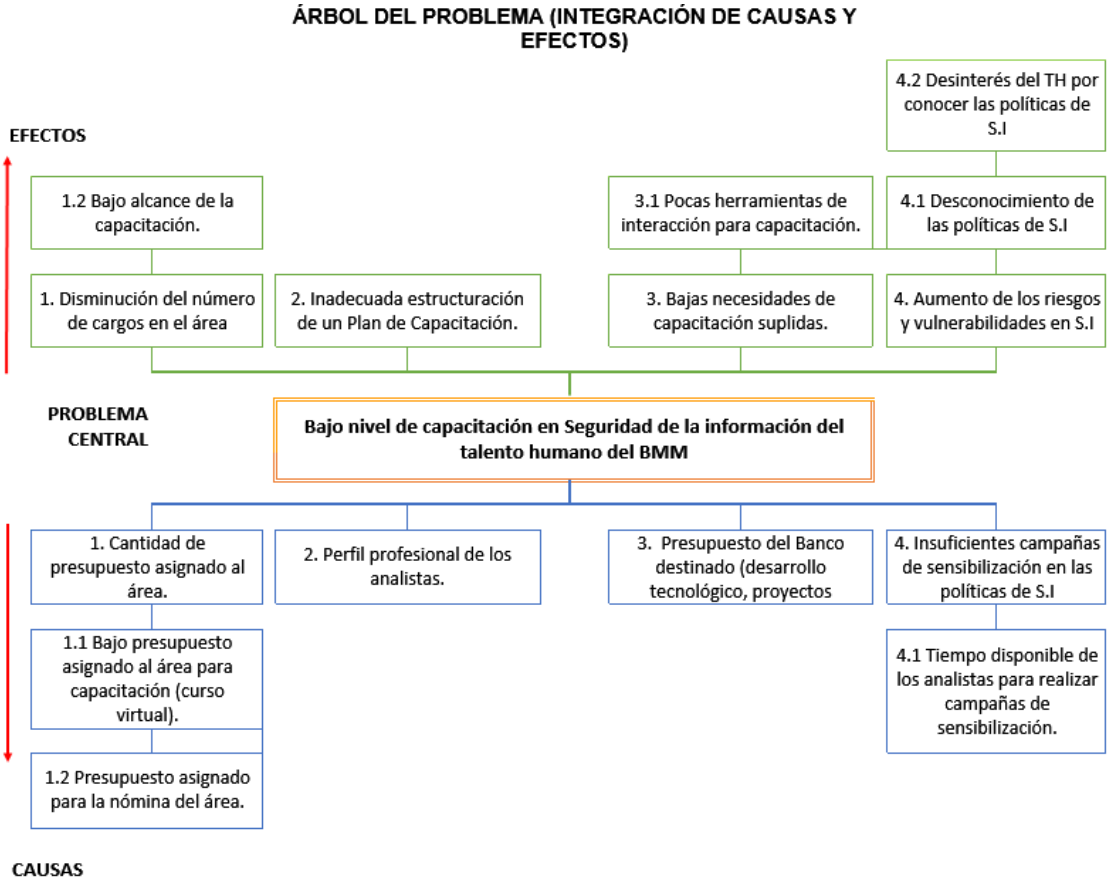


Figura 13. Árbol del Problema

La matriz de riesgos de seguridad de la información (**¡Error! No se encuentra el origen de la referencia.**) deja en evidencia los principales riesgos en materia de seguridad que se podrían presentar según los procesos del área de S.I, los cuales son:

1. Sustracción de información confidencial de la entidad (Fraude Interno).
2. Accesos no autorizados sobre las bases de datos internas a través de los superusuarios.
3. Accesos no autorizados sobre los portales transaccionales a través del perfil de superusuarios de las entidades.
4. Fuga de información.
5. Explotación de vulnerabilidades y/o debilidades sobre los sistemas de información.
6. Perdida de información, producto de infección por virus informático.

Tabla 5. Matriz de Riesgo del Área de Seguridad de la Información

PROCESO	RIESGO	CAUSA	FACTOR DE RIESGO	RIESGO INHERENTE / RIESGO INHERENTE	RIESGO RESIDUAL - / RIESGO RESIDUAL
IT-002 Clasificación de la información PR-017 Administración de Usuarios.	Sustracción de información confidencial de la entidad (Fraude Interno)	Deficiencias en la aplicación de la metodología para la clasificación de la información.	Procesos	Alto	BAJO
		Accesos no autorizados a los diferentes aplicativos	Procesos		
		Falta de segregación de funciones.	Procesos		
PR-017 Administración de Usuarios. PR-034. Gestión de usuarios sensitivos. PT-007 Políticas de seguridad de la información	Accesos no autorizados sobre las bases de datos internas a través de los superusuarios.	Cambios no autorizados sobre las contraseñas de los usuarios sensitivos.	Procesos	Moderado	BAJO
		Fallas en el seguimiento y control del préstamo de las contraseñas de usuarios sensitivos.	Procesos		
		No hacer la debida identificación y segregación de usuarios sensitivos (ROOT/Admin)	Procesos		
		Administración inadecuada de servicios con usuarios sensitivos	Procesos		
		Deficiencias en la generación y no renovación frecuente de las contraseñas de usuarios sensitivos	Recurso Humano		
PR-062 Portales Bancarios	Accesos no autorizados sobre los portales transaccionales a través del perfil de superusuario de las entidades.	Concentración de atribuciones en el usuario administrador de los portales bancarios	Recurso Humano	Moderado	BAJO
PR-081 Aseguramiento de infraestructura tecnológica PR-017 Administración de usuarios. PT-007 Seguridad de la información (listas blancas) PR-056 Administración de activos de Hardware y Software	Fuga de información	Acceso no autorizado a los repositorios de información	Recurso Humano	Moderado	BAJO
		Robo y/o pérdida de equipos de computo	Externos		
		Remitir correos electrónicos a destinatarios externos no autorizados.	Recurso Humano		
PR-081 Aseguramiento de infraestructura tecnológica PR-038 Gestión de servicio de tecnología PR-086 Gestión de vulnerabilidades	Explotación de vulnerabilidades y/o debilidades sobre los sistemas de información	Desactualización de las herramientas de análisis (Retina)	Tecnología	Moderado	BAJO
		Desconocimiento por parte del personal a cargo de la identificación de vulnerabilidades	Recurso Humano		
		La herramienta no tiene cobertura sobre los activos de información a analizar	Tecnología		
		Diseño y/o implementación inadecuada de medidas y mecanismos de seguridad	Tecnología		
		Saturación del canal de comunicación por realizar escaneos de vulnerabilidades en horarios hábiles	Tecnología		
PT-007 Política de seguridad de la información. PR-038 Gestión de servicio de tecnología	Pérdida de información producto de infección por virus informático.	Fallas en la administración del sistema antivirus.	Recurso Humano	Moderado	BAJO
		Desconocimiento en el manejo de adjuntos por parte de los usuarios finales.	Recurso Humano		

Fuente: Área de Riesgo Operativo

Una vez inventariados los niveles de riesgo en seguridad de la información del área, se define en consenso con el grupo de trabajo los principales riesgos en S.I a nivel organizacional, los

cuales son el **fraude interno, las fugas y perdidas de información por virus informático**, teniendo en cuenta los anterior se definieron 4 principales necesidades de capacitación en seguridad de la información, estas son:

1. Conocimientos generales de seguridad de la información.
2. Conocimiento e Identificación de las principales vulnerabilidades de Seguridad de la información.
3. Manejo de Información Confidencial.
4. Conocimiento de las Políticas de Seguridad de la Información.
5. Gestión de la Información.

1.2.1 Abaco de Regnier

Para delimitar el contenido del programa capacitación se utiliza la herramienta del Abaco de Regnier la cual tiene como fin interrogar al grupo de trabajo sobre su opinión acerca de las necesidades establecidas, de la siguiente manera:

Se le explico a cada integrante del grupo de expertos, las necesidades de capacitación establecidas.

A. Conocimientos generales sobre seguridad de la información: Dar a conocer conceptos, responsabilidades, elementos de S.I, normatividad.

B. Conocimiento e Identificación de las principales vulnerabilidades de Seguridad de la información: Capacitar sobre las vulnerabilidades existentes en los sistemas de información, como walmare, virus, ataques cibernéticos, Phishing.

C. Manejo de Información Confidencial: Capacitar acerca de la clasificación de la información según los criterios establecidos de confidencialidad, integridad y disponibilidad.

D. Conocimiento de las Políticas de Seguridad de la Información: Incluir las políticas de seguridad de la información más relevantes como: Uso de contraseñas, Uso de internet, Uso del servidor de archivos y Uso del correo electrónico.

E. Gestión de la información, incluir en la capacitación los derechos del titular de la información y deberes de quienes la administran (PT. 029 Protección de datos personales).

1.2.1.1 OPINIÓN DE EXPERTOS

Con base en la siguiente ficha, cada uno de ellos expreso su opinión según la clasificación de la .

.

Tabla 6. Opinión de Expertos

OPINIÓN	COLOR	SIGNIFICADO
R		No incide
r		Incide muy poco
A		Neutro
v		Incide algo
V		Incide Mucho
B		Participa sin opinión
N		No participa

La ficha individual, incluye la pregunta:

Teniendo en cuenta la estructuración de un plan de capacitación y sensibilización para reducir los riesgos de seguridad de la información ¿Cómo incide incluir las siguientes necesidades de capacitación en este plan?, como se muestra en la Figura 14.

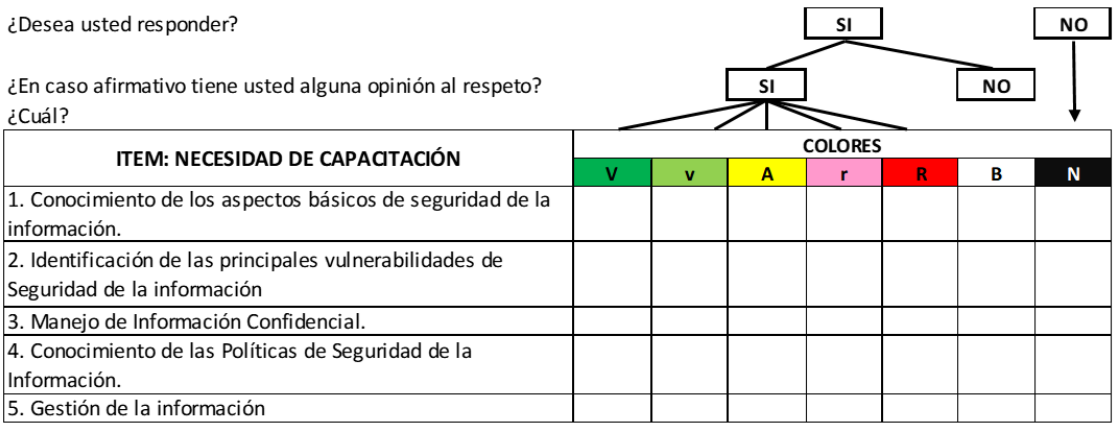


Figura 14. Aplicación del Abaco de Regnier

1.2.1.2. ANALISIS DE ABACO DE REGNIER

La respuesta de los 4 expertos, se encuentra en el ANEXO 5. Evidencias, y se agrupo como se ilustra en la Tabla 7:

EXPERTOS:

A. Marcela Solano- Analista S.I.
B. Victoria Martínez- Analista Riesgo Operativo.
C. Juan Pablo Rodríguez- Gerente de Riesgos no financieros.
D. Carlos Rodallega-Especialista en S.I.

Tabla 7. Análisis del Abaco de Regnier

ITEM: NECESIDAD DE CAPACITACIÓN	EXPERTOS			
	A	B	C	D
1. Conocimiento de los aspectos básicos de seguridad de la información.	v	A	V	V
2. Identificación de las principales vulnerabilidades	v	V	V	V
3. Manejo de Información Confidencial.	r	A	V	v
4. Conocimiento de las Políticas de Seguridad de la Información.	V	V	V	V
5. Gestión de la información	v	v	R	V

La opinión de los 4 expertos se agrupo según las necesidades de capacitación que tienen mayor incidencia, como se ilustra en la Tabla 8 .

Tabla 8. Resultados Agrupados del Abaco de Regnier

ITEM: NECESIDAD DE CAPACITACIÓN	OPINIONES			
1. Conocimiento de las Políticas de Seguridad de la Información.	V	V	V	V
2. Identificación de las principales vulnerabilidades	V	V	V	v
3. Conocimiento de los aspectos básicos de seguridad de la información.	V	V	v	A
4. Gestión de la información	V	v	v	R
5. Manejo de Información Confidencial.	V	v	r	A

1.2.2 Necesidades de capacitación

Partiendo del análisis de los expertos se concluye que todas las necesidades de capacitación detectadas deben suplirse mediante capacitación y sensibilización, sin embargo considerando que la necesidad (3) conocimiento en aspectos de SI, y la gestión de la información (4) por parte de los usuarios puede suplirse mediante estrategias de sensibilización y que la necesidad del manejo de información confidencial (5) está dirigida principalmente a los jefes y gerentes de área, se definieron dos necesidades específicas de capacitación, a saber:

1. El conocimiento de las principales políticas de Seguridad de la Información establecidas.
2. La identificación de vulnerabilidades de los sistemas de información por parte de los colaboradores.

Con base en estas necesidades se definición en consenso con el grupo de expertos las siguientes temáticas de capacitación:

Tabla 9. Temáticas de Capacitación

NECESIDAD DE CAPACITACIÓN	TEMÁTICA
1. Conocimiento de las Políticas de Seguridad de la Información.	1. Uso de contraseñas
	2. Uso del correo electrónico.
	3. Buen uso de internet.
	4. Seguridad para los dispositivos USB.
	5. Uso y control de portátiles
	6. Escritorio y Pantalla Limpia
	7. Uso del Servidor de archivos
2. Identificación de las principales vulnerabilidades de Seguridad de la información	8. Ciberseguridad
	9. Malware Protección contra los virus.
	10. Rasomware
	11. Phishing

2. OBJETIVOS Y ALCANSE DEL PLAN

2.1 OBJETIVO GENERAL

Establecer los lineamientos que orienten la capacitación y sensibilización en Seguridad de la Información para el talento humano del banco, con base en las Políticas Internas de Seguridad de la información establecidas.

2.2 OBJETIVOS ESPECIFICOS

1. Incrementar los conocimientos sobre las Políticas de Seguridad de la información establecidas en el BMM.
2. Reducir los riesgos de seguridad de la información asociados a la perdida de información producto de virus informático.
3. Realizar campañas de sensibilización sobre seguridad de la información a través de mailings.
4. Establecer las orientaciones conceptuales, pedagógicas y temáticas para la capacitación en seguridad de la información.
5. Contribuir a la formación del talento humano del Banco, en el reconocimiento de vulnerabilidades en los sistemas de información.

3. CONTENIDO DEL PLAN DE CAPACITACIÓN

3.1 ASPECTOS GENERALES

El Banco Mundo Mujer, se ha propuesto implementar un esquema de seguridad de la información, el cual le permitirá gestionar efectiva y constantemente la confidencialidad, confiabilidad, eficiencia, integridad, disponibilidad y cumplimiento, sobre sus activos de información, lo anterior siguiendo los lineamientos propuestos por el estándar ISO 27001:2013.

¿Qué es Seguridad de la Información?

La Seguridad de la información consiste en proteger los activos de información del Banco Mundo Mujer de una posible perdida, daño, destrucción o robo.

¿Cuáles son los activos de información?

Figura 15. Activos de Información

¿Cuál es la responsabilidad de los usuarios?

- ✓ Los colaboradores del Banco deben proteger los activos de información de la Entidad.
- ✓ Los colaboradores deben asegurar la confidencialidad de la información, de tal manera que únicamente los usuarios autorizados tengan acceso.
- ✓ Los colaboradores del Banco deben mantener la integridad de la información, evitando su alteración no autorizada.
- ✓ Los colaboradores del Banco, deben tener disponibilidad de la información, asegurando su presencia cuando sea requerida por usuarios debidamente autorizados y en un tiempo razonable de respuesta.

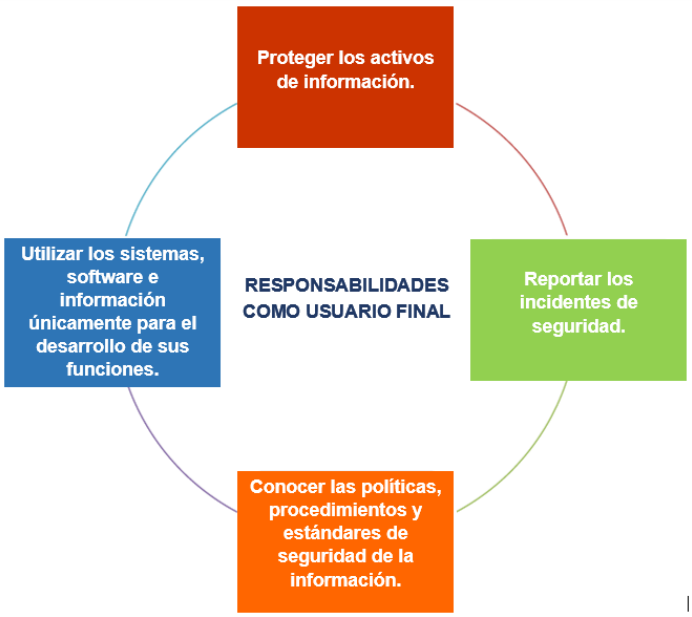


Figura 16. Responsabilidad de los Usuarios Finales

¿Cuáles son los elementos de la seguridad de la información?

Tabla 10. Elementos básicos de la Seguridad de la Información

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
Propiedad de la información que no se revela ni se encuentra a disposición de individuos, organizaciones o procesos no autorizados.	La propiedad de salvaguardar la exactitud y completitud de los activos.	Propiedad que puede ser accesible y utilizable ha pedido de un agente autorizado.

MANEJO DE INFORMACIÓN CONFIDENCIAL, RESTRINGIDA E INTERNA.

Tabla 11. Niveles de Clasificación de la Información.

CONFIDENCIAL	Información muy sensible que en caso de ser revelada sin autorización, impacta negativamente a la organización (Datos de clientes, claves de acceso).

RESTRINGIDA	Información interna de las operaciones del Banco, esta no debe ser divulgada en la organización.
USO INTERNO	Información que puede ser divulgada dentro de la organización, pero causa un impacto negativo si es divulgada externamente.
PÚBLICA	Información no clasificada, toda la información que no se incluya en las anteriores clasificaciones se considera pública, esta puede ser divulgada sin causar ningún impacto negativo en la organización.

¿Qué debe hacer, quienes manejan información?

Para proteger la confidencialidad, integridad y disponibilidad de la información usted debe:

1. Copias de la información Confidencial, Restringida e Interna: Se debe firmar un acuerdo de confidencialidad con terceras partes, en caso de requerir entregar información electrónica o escrita confidencial, restringida o interna, con las restricciones de su uso.

2. Destrucción de Información Confidencial, Restringida e Interna: Se debe borrar la información confidencial, restringida o interna, de los medios magnéticos de manera que no sea recuperable en el momento de deshacerse de estos elementos. En caso de información impresa se deben utilizar mecanismos que impidan volver a recuperar los documentos.

3. Impresión de Información Confidencial, Restringida e Interna: Información clasificada como confidencial, restringida o interna, no debe ser enviada a la impresora sin que haya una persona autorizada para su recuperación, garantizando su confidencialidad durante y después de la impresión.

4. Transmisión por medios electrónicos de información Confidencial, Restringida e Interna: La información que sea catalogada como confidencial, restringida e interna que requiera ser transmitida por medios de comunicación públicos, debe ser cifrada con el fin de proteger su confidencialidad.

3.2 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

El contenido de la capacitación incluye explicar las políticas más relevantes de Seguridad de la Información establecidas por el área.

3.2.1 Uso de contraseñas

El usuario y contraseña es de uso personal e intransferible, por lo tanto no se debe suministrar, compartir, escribir o divulgar a través de correo electrónico u otros medios a ningún funcionario o personal externo de la Institución. Las contraseñas en los sistemas de información deberán cumplir con las siguientes características:

- ✓ Contener mínimo 8 y máximo 10 caracteres.
- ✓ Utilizar números, letras y símbolos especiales.
- ✓ No utilizar el nombre de usuario asociado.
- ✓ No repetir los mismos caracteres en la misma contraseña. (ej.: “111222”).
- ✓ No se puede utilizar secuencias básicas de teclado, por ejemplo: “qwerty”, “abcde” o en numeración: “1234” ó “98765”).

Los usuarios deben cambiar las contraseñas genéricas que les han sido asignadas cuando ingresen a los sistemas de información, y debe ser actualizada cada 30 días, teniendo en cuenta que no se puede utilizar una de las seis (6) últimas contraseñas registradas.

El colaborador debe recordar que cuando se presenten más de (5) intentos fallidos en el acceso a un sistema de información, el usuario será bloqueado por un lapso de (1) una hora.

3.2.2 Uso del correo electrónico institucional

Los colaboradores deben ser conscientes de que el correo electrónico institucional es de uso laboral, el nombre de usuario y contraseña es personal e intransferible; además, el correo

electrónico institucional no debe ser inscrito en redes sociales o cualquier tipo de blog que no sea de gestión diaria del cargo. Algunas restricciones son:

- ✓ No se puede suministrar el correo institucional para asuntos de índole personal tales como suscripciones a revistas, recepción de publicidad de cualquier tipo, u otro ámbito que no tenga relación con el desempeño de sus funciones.
- ✓ La distribución de correos electrónicos tipo SPAM está totalmente prohibida dentro de la empresa, esto puede afectar la continuidad del servicio de correo electrónico.
- ✓ El envío de correos a los grupos institucionales, los funcionarios solo tendrán permisos de envío a los correos que se ajusten al perfil de su cargo; la única área facultada para comunicarse con todos los funcionarios de la Institución será Mercadeo.
- ✓ El envío de información de la compañía a correos electrónicos diferentes a los de la institución.
- ✓ La capacidad de envío de documentación adjunta; esta dependerá del perfil del cargo que ostente el funcionario de la Institución.

Entre las responsabilidades sobre el uso del correo institucional se encuentran:

- ✓ El uso del correo institucional fuera de las instalaciones de la entidad de manera responsable por parte del funcionario, el Banco no se hace responsable por el robo de contraseñas o acceso de personas ajenas a la cuenta.
- ✓ Todo funcionario de la Institución que cuente con una dirección de correo electrónico tiene la responsabilidad de implementar su firma de correo según el estándar definido por la institución; esta deberá ser utilizada para enviar o responder los correos electrónicos.

Además de las restricciones y responsabilidades sobre el uso del correo institucional se debe tener en cuenta que:

1. Los correos electrónicos que los funcionarios requieran remitir con asuntos correspondientes a observaciones, reclamos y/o solicitudes laborales deben seguir el orden jerárquico establecido; informando en primera instancia a su superior inmediato, antes de escalar la petición a niveles superiores.

2. Las conversaciones, correos electrónicos e incluso la navegación a través de internet podrán ser sujeto de auditorías aleatorias para verificar el cumplimiento de las políticas de uso de correo electrónico.

3. Los siguientes cargos no tienen asignado correo institucional:

- Aprendices SENA
- Cajeros
- Auxiliar de Servicios
- Auxiliar de Servicios Generales
- Analistas de Crédito, exceptuando a los analistas de pequeña empresa
- Asesores de Servicio
- Coordinadores de Operaciones
- Analistas de Operaciones

4. Las Gerencias serán las únicas facultadas para solicitar la creación de correos electrónicos genéricos, previo soporte de los motivos de la petición; la solicitud debe contar con la aprobación del Área de Seguridad de la Información para que sea implementada.

3.2.3 Buen uso de internet

Debido a los riesgos de seguridad de la información que representa el uso del servicio de internet dentro de la institución, existen las siguientes restricciones:

- ✓ Cualquier actividad que infrinja o haga un uso inapropiado de los derechos de propiedad intelectual de un tercero, como copyright, marcas registradas, secretos comerciales, piratería de software, patentes, etc.
- ✓ La búsqueda y navegación por páginas web con contenido pornográfico, redes sociales, racismo, juegos, entre otros.
- ✓ El acceso a los portales de correo electrónico personal (Hotmail, Gmail, Yahoo, entre otros.).
- ✓ El uso de portales y/o aplicaciones para almacenar información en la nube (Dropbox, Skydrive, Google Drive, iCloud, entre otros).
- ✓ La búsqueda, navegación y reproducción de contenido multimedia por ejemplo escuchar música y ver vídeos, entre otros.

- ✓ La descarga de Software, programas o aplicaciones de cualquier tipo.
- ✓ El uso de aplicaciones de búsqueda (kazaa, e-mule, Ares, Imesh, P2P, limeware, entre otros) para la obtención de archivos comerciales, música o videos con derechos reservados.
- ✓ Publicar información gráfica, fotos, videos, música, entre otros, que sea difamatoria, escandalosa, privada o que infrinjan estrés emocional sobre una persona o que atente contra la honra, moral, ética, dignidad y buen nombre de la Institución.

Se debe tener en cuenta que la navegación en internet, en la Institución, está limitada de acuerdo a las funciones definidas para cada cargo.

3.2.4 Seguridad para los dispositivos USB.

Los dispositivos USB representan uno de los mayores riesgos de seguridad de la información, que es el fraude interno, ya que permiten fácilmente la sustracción de información confidencial del Banco, para ello se establecieron las siguientes políticas:

1. Los Vicepresidentes y Gerentes serán los únicos autorizados para el uso de medios de almacenamiento masivo USB en la Dirección General, los cuales sólo tendrán permisos de LECTURA.

2. Los colaboradores del Banco tienen restricción de puertos USB para el uso medios de almacenamiento masivo, con el fin de evitar fuga de Información (fraudes), ingreso de virus, malware indeseado y pérdida de información confidencial.

3. Se habilitan permisos de LECTURA a funcionarios de la dirección general, siempre y cuando las solicitudes justifiquen la necesidad y expliquen de manera detallada por qué y cuánto tiempo requieren el permiso.

4. Los Vicepresidentes y Gerentes serán responsables de las solicitudes de habilitación de puertos USB para algún funcionario a su cargo; los permisos otorgados solo corresponderán a lectura de dispositivos de almacenamiento masivo.

Si el funcionario requiere necesariamente la utilización de un dispositivo USB, es el área de Seguridad de la Información y Continuidad del Negocio, es la responsable de autorizar las solicitudes de habilitación de puertos USB; Una vez aprobada el área de Tecnología Informática realiza la activación correspondiente.

3.2.5 Uso y control de portátiles

Este tipo de equipo solo está asignado formalmente a los siguientes cargos: Presidencia, Vicepresidentes, Gerentes, Jefes de áreas, Coordinadores y Áreas de control; en caso de que un funcionario tenga que realizar labores fuera de las instalaciones se le asignará un computador portátil temporal.

Cada portátil asignado tiene carácter intransferible y es responsabilidad del funcionario a quien se le asigno, por tanto no se puede realizar préstamos de este equipo. El funcionario debe tener en cuenta que:

1. Las especificaciones técnicas del computador portátil se determinarán de acuerdo al tipo de programas de aplicación que el usuario necesite para el desarrollo de sus funciones

2. Los usuarios a quienes se han asignado equipos portátiles están en el deber de solicitar periódicamente al área de Tecnología Informática la actualización del software antivirus.

3. Los funcionarios que tengan asignado cualquier equipo de tipo portátil, deben hacer correcto uso de los mismos y de la información que contienen; debido a las características de ese tipo de tecnología, se presentan más vulnerabilidades de seguridad, por las facilidades de conectarse en diferentes ambientes informáticos, en los cuales la institución no tiene control, y adicionalmente son más susceptibles a robo o pérdida.

4. Las conexiones a red por fuera de las instalaciones del Banco Mundo Mujer se harán exclusivamente a través de la VPN (Virtual Private Network) que configure el área de Tecnología Informática.

5. Los funcionarios de la institución deben cumplir con las siguientes recomendaciones:

- ✓ Mantener el computador siempre a la vista y no dejarlo desatendido.
- ✓ Tener especial cuidado en los medios de transporte público y aeropuertos.
- ✓ Usar maletines o morrales que no indiquen que se lleva un portátil.
- ✓ No enviar el equipo nunca como equipaje de bodega.
- ✓ En los hoteles si se tiene que dejar el equipo, asegurarlo en recepción o cajillas de seguridad de ser posible.
- ✓ Contar con algún mecanismo de encriptación de la información del negocio.

3.2.6 Escritorio y pantalla limpia

Con el fin de mantener la seguridad de la operación en la Institución todo funcionario debe mantener la información física y digital protegida o no disponible en los tiempos que no se encuentre en su puesto de trabajo, bloqueando su sesión. Por lo tanto con el fin de supervisar la efectividad de la política todos los empleados serán los encargados de reportar su incumplimiento de esta manera:

- ✓ Recolectar la evidencia necesaria para justificar el incumplimiento y entregarla al jefe inmediato, por ejemplo:
- ✓ Fotografía.
- ✓ Video.
- ✓ Elemento causante de la infracción.
- ✓ Enviar un correo a infoseguridad@bmm.com.co con copia al jefe inmediato, con la siguiente información: Nombre del infractor, cargo, área, agencia/PDA y ciudad.

El Gerente o jefe de área tiene la responsabilidad de diseñar sanciones de tipo educativo, Como por ejemplo:

- ✓ Dinámicas lúdicas como elaborar una presentación o cartelera relacionada con la seguridad de la información y presentarla ante sus compañeros de trabajo, lo cual se realizará en horario de 7:00 a.m. 7:45 a.m.
- ✓ Compartir un pasabocas con los compañeros de Agencia o área.
- ✓ Dentro de las áreas, y agencias existe un líder, encargado de apoyar la implementación de la política.

AREA DE TRABAJO SEGURA

En cada área se requiere que se cumpla con las Políticas de Seguridad de la Información establecidas, por lo cual todos los empleados y terceros involucrados (proveedores) tienen la responsabilidad de asegurar su espacio de trabajo, guardando la información confidencial y la información restringida en un lugar apropiado, cerrar con llaves las gavetas y gabinetes, bloquear el computador personal al moverse del escritorio y apagar sus equipos al final del día.

¿Qué debo hacer?

Al moverse o ausentarse de su área de trabajo debe asegurarse de proteger,

1. Información clasificada como confidencial y restringida.
2. El computador personal, bloqueando su acceso.
3. Agendas electrónicas y celulares.

3.2.7 Uso del Servidor de archivos

El servidor de archivos únicamente se encuentra autorizado para el almacenamiento de información relacionada con las actividades laborales y funciones asignadas, propias de cada cargo.

¿Cómo hacer uso adecuado del servidor de archivos?

Cada gerencia cuenta con una carpeta dentro del servidor de archivos en la cual se almacena toda la información crítica de los procesos y actividades del quehacer diario de los funcionarios, estos deben tener en cuenta que:

1. Es cada funcionario el responsable del manejo y cuidado de la información almacenada en el servidor de archivos.
2. En el servidor de archivos no debe ser almacenada información personal tales como documentos, archivos de imagen, videos, música y ejecutables; igualmente archivos inapropiados o potencialmente ofensivos.
3. El servidor de archivos contará con dos grupos de control de carpetas:

    - ✓ Permiso de Lectura y/o Escritura: Funcionarios del área, sobre las carpetas que les sean de su competencia.
    - ✓ Permiso de Lectura: Demás funcionarios de la Institución, sobre las carpetas a las cuales se les autorice el acceso.

¿Cómo función la Carpeta Pública?

El servidor de archivos cuenta con una carpeta pública, a la cual se puede acceder desde cualquier punto de la organización, sin restricciones de lectura o escritura. La información que sea almacena en la Carpeta Pública no cuenta con un plan de Backup por tratarse de un medio de intercambio de información temporal, por lo tanto sólo podrá ser usada como un medio de transferencia de archivos o almacenamiento temporal de información.

Los archivos almacenados en la Carpeta Pública no hacen parte del plan de restauración de archivos, por esto los documentos almacenados dentro de esta carpeta serán eliminados diariamente al final de la jornada por la Gerencia de Tecnología Informática.

Cada funcionario debe tener en cuenta los siguientes aspectos, al hacer uso del servidor de archivos:

1. El Jefe de cada área es responsable de realizar periódicamente seguimiento y control sobre la información almacenada en el servidor correspondiente a su área.

2. Cuando la información se considere inadecuada, se indaga por el responsable directo y se informa al área de Seguridad de la Información y a la Gerencia Talento Humano para que se tomen las medidas pertinentes.

3. Todos los documentos almacenados en el servidor de archivos son propiedad de la Institución.
4. El área de Seguridad de la Información es la única autorizada para aprobar la creación de carpetas en el servidor de archivos; igualmente será responsable de definir los permisos de acceso y control de las mismas.

5. La Gerencia de Tecnología es la única encargada de administrar los permisos de acceso autorizados por el área de Seguridad de la información.

3.3 VULNERABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

CIBERSEGURIDAD

¿Porque Ciberseguridad?

1. Norma ISO/IEC 27032:2012
2. **Requerimiento *"Circular Externa 007 de 2018"* de la SFC**
3. Servicios expuestos
    - Correo
    - Lync
    - Página Web
    - *App Móvil*
    - *Web transaccional*
    - Acceso a servicios en el ciberespacio
    - Navegación web
    - SFTP.

La definición de ciberseguridad por parte de ISACA (Information Systems Audit and Control Association – Asociación de Auditoría y Control sobre los Sistemas de Información) es la "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados".

La norma ISO 27001 define activo de información como los conocimientos o datos que tienen valor para una organización, mientras que los sistemas de información comprenden a las aplicaciones, servicios, activos de tecnologías de información u otros componentes que permiten el manejo de la misma

Por lo tanto, la ciberseguridad tiene como objetivo la protección de la **información digital** que se encuentra en los sistemas interconectados y está comprendida dentro de la seguridad de la información.

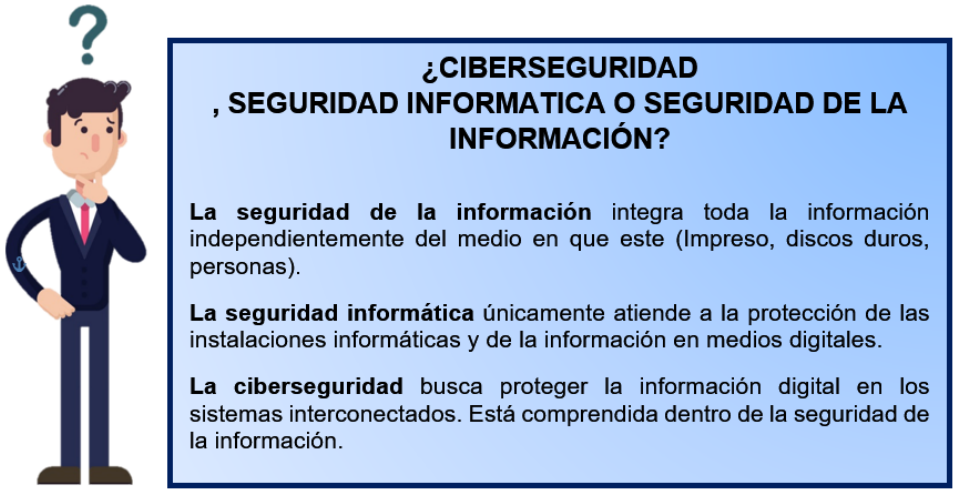


Figura 17. Ciberseguridad, Seguridad Informática y Seguridad de la Información.

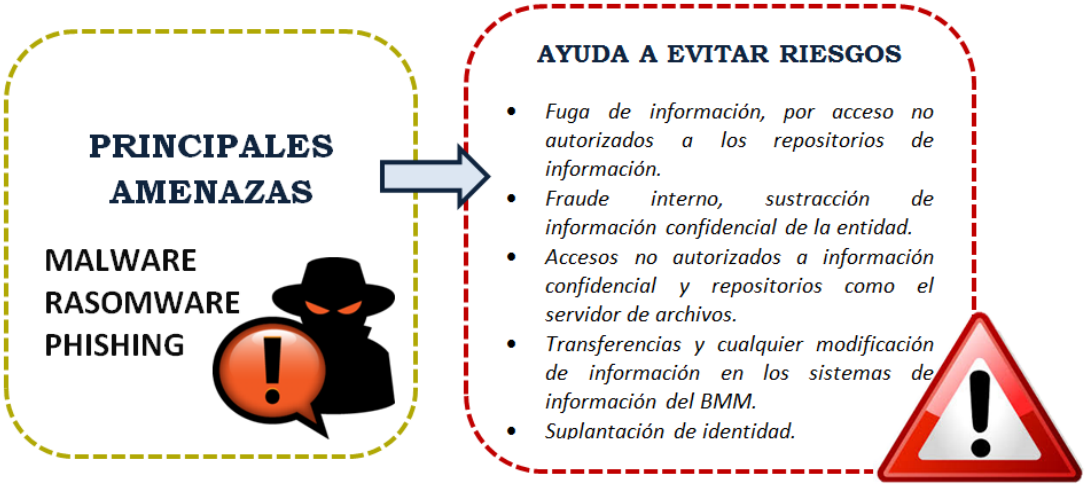


Figura 18. Principales Amenazas de Los Sistemas de Información

3.3.1 Malware

- **¿Qué es el Malware?**

Malware (malicious software), también llamado badware, se utiliza para referirse a cualquier software malicioso que tiene como objetivo infiltrarse y causar daño en el quipo o Sistema de información.

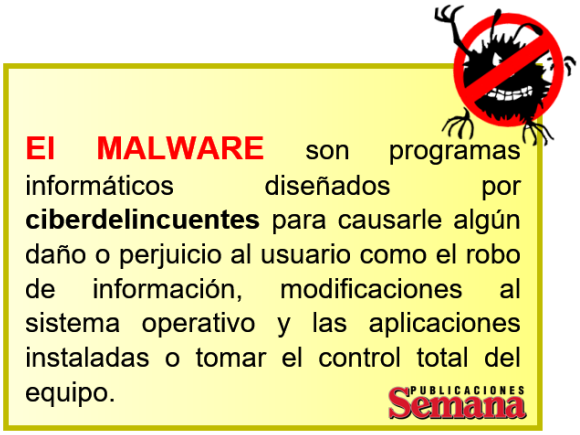


Figura 19. Definición de Malware

El Diagnostico para Latinoamérica realizado por ESET Latinoamérica, (ESET Security Report 2017_ Enjoy Safer Technology), indican que la evolución de los incidentes de seguridad

relacionados con malware desde 2009 hasta 2016, han aumentado desde un 39% en 2014 hasta un 49% en el 2016, como se ilustra en la Figura 20, presentándose una tendencia creciente, debido en gran medida a la cantidad de códigos maliciosos que se desarrollan en la actualidad, los métodos empleados para su propagación y las ganancias económicas que obtienen los cibercriminales que los desarrollan y/o financian.

- **Como actúa el Malware**

DISPOSITIVOS USB: Las políticas de Seguridad de la información incluyen la restricción de puertos USB como medios de almacenamiento masivo, y autoriza a algunos colaboradores como: Vicepresidentes y gerentes, Analista Agropecuarios.

CORREO ELECTRÓNICO: El funcionario puede recibir un correo aparentemente confiable (proveedor, cliente, entidad financiera) con archivos adjuntos (fotos, documentos, música, ejecutables de virus), convirtiéndose en la forma más efectiva y utilizada para transmitir y propagar el malware.

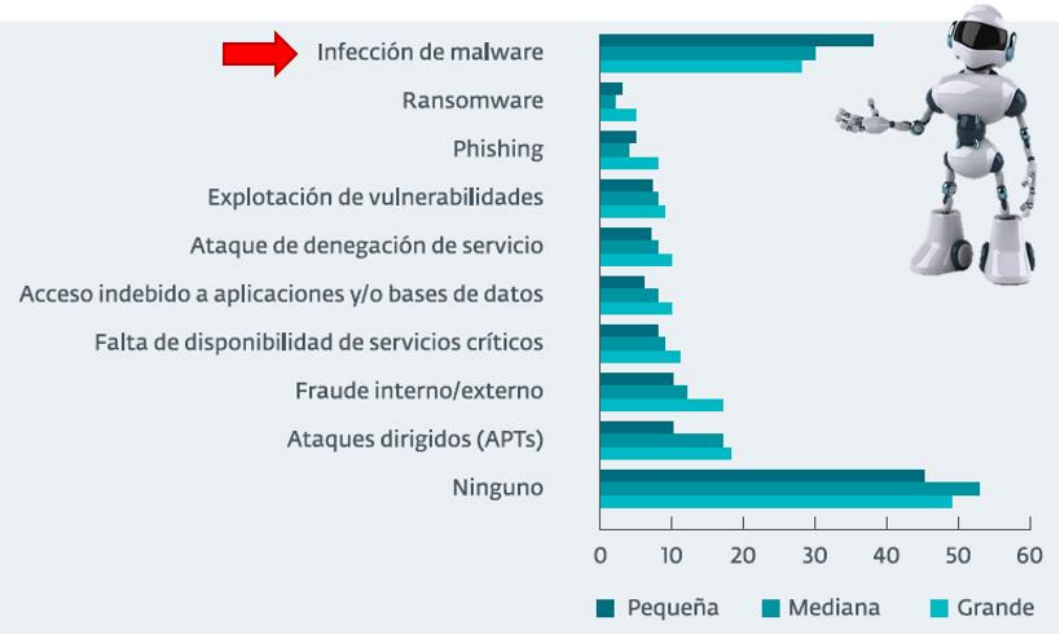


Figura 20. Incidentes de Seguridad Relacionados con Malware.

DESCARGAS: El Malware puede afectar el equipo a través de la descarga de un archivo, aplicación o software, por lo cual cada empleado del Banco debe recordar la política sobre uso

de internet que establece que se encuentra prohibido, La descarga de Software, programas o aplicaciones de cualquier tipo.

- **Tipos de Malware**

El malware puede ser principalmente de tres tipos:

VIRUS: Término estándar para nombrar a un software malicioso, que busca alterar el funcionamiento normal de nuestro equipo; su característica principal es que al ejecutarse propaga infectando otros softwares ejecutables (se reproduce así mismo) dentro de la misma computadora.

El virus pasa a extenderse por otros ejecutables del sistema, algunos afectan archivos de Word o Excel. Un ejemplo de virus son MyDoom, Melisa, CryptoLocker, Vawtrak, love you.

Uno de los primeros virus conocidos es Melisa, archivo de Word que decía tener contraseñas de accesos a sitios pornográficos, este virus infecto las computadoras además de que se reenviaba a los contactos de **correo electrónico.**

GUSANO: Código malicioso diseñado para propagarse automáticamente a través de cualquier medio como dispositivos de almacenamiento USB, discos duros, redes corporativas.

Es un malware que actúa individualmente, no requiere ejecución del usuario para reproducirse y no infectan archivos existentes para difundirse.

Algunos ejemplos de este tipo de malware son el Gusano Sasser, Blast.

Sasser es un gusano que se propaga a través de Internet, el virus se extendió por la red de informática, en busca de ordenadores con sistemas operativos Windows 2000 y XP sin actualizar. El gusano Sasser; Microsoft alertó de la existencia de este problema en Windows 2000 y XP, pero muchos usuarios todavía no han instalado el correspondiente parche.

A diferencia de la mayoría de los virus, Sasser no necesita que el usuario pinche en un fichero para activarse. Además, este gusano es capaz de escanear automáticamente la red en busca de los ordenadores con esta vulnerabilidad, según expertos informáticos (Fuente: El Tiempo, 2004).

El virus afectó al banco finlandés Saffo, que hoy tuvo que cerrar 120 oficinas durante unas horas para poner al día sus sistemas de seguridad.

TROYANO: Su característica principal es que simula ser un programa autentico como un software gratuito o un programa legítimo que puede hasta permitir la entrada al equipo de forma remota sin ser detectado, logrando robar datos, archivos e instalar otros tipos de malware.

Un ejemplo de este virus es el Bayrob, el cual durante enero de 2016 se detectó en auge en países como Argentina, Chile, Colombia y Ecuador**. Una** forma de propagación es a través de un correo electrónico notificando al usuario que ha recibido algún tipo de beneficio o vale, con el cual se invitaba a la víctima a descargar un archivo adjunto para obtener el supuesto beneficio.

Bayrob es un troyano utilizado por los atacantes como un backdoor y puede ser controlado remotamente. Tiene la capacidad de enviar información del sistema en que se encuentra (pueden expiar nuestras búsquedas en internet) y la lista de procesos que actualmente estén corriendo, así como de actualizarse a una nueva versión, descargar y ejecutar archivos. (FUENTE: WeliveSecurity ESET).

3.3.2 Rasomware

- **¿Qué es el Rasomware?**

El Rasomware es un software malicioso infecta nuestro equipo, permitiéndole a un ciberdelincuente secuestrar nuestro equipo (información) de manera remota y encriptar nuestra información, este virus lanza una ventana emergente en la que nos pide el pago de un rescate, por lo general en moneda virtual (bitcoins por ejemplo).

- **Ejemplos de Rasomware**

Fuente: El Espectador, Mayo 2017

Son 37 casos reportados ante el Centro Cibernético de la Dijín de la Policía por la afectación del virus Wannacry, el mismo que ha secuestrado la información de más de 200.000 sistemas en empresas, entidades gubernamentales, hospitales, bancos y universidades de 120 países y

que pide un rescate de alrededor de US$300 para recuperarla. Según el director de este centro, coronel Fredy Bautista, el programa maligno, principalmente, llegó de forma masiva a Colombia **a través de un correo sospechoso que tenía como asunto "Transferencia banca en línea"** y como remitente tenía una entidad financiera mexicana.

La forma como funciona Wannacry es simple, se descarga el virus a través de un archivo adjunto, que puede ser un PDF o un documento de Word o Excel, luego aparece un mensaje de error, que informa una supuesta anomalía en el sistema. Inmediatamente se le da cerrar a esa ventana, aparece una especie de programa en el que hay dos relojes que hacen la cuenta regresiva**.** El primero es de tres horas, tiempo que se le da a la víctima para que pague US$300 en bitcoins. De no hacerlo, la cifra sube a US$600 y ya le quedan solamente 24 horas para evitar la pérdida de la información.

3.3.3 Phishing

- **¿Qué es el Phishing?**

El Phishing es un engaño difundido por la rede el cual un ciberdelincuente denominado phisher, suplanta la identidad de una persona o empresa de confianza utilizando el correo electrónico, para obtener información confidencial o infectar el equipo.

El término Phishing viene del inglés fishing, que significa pescar, haciendo referencia a pescar datos personales como nombres de usuario, contraseñas o datos de cuentas bancarias.

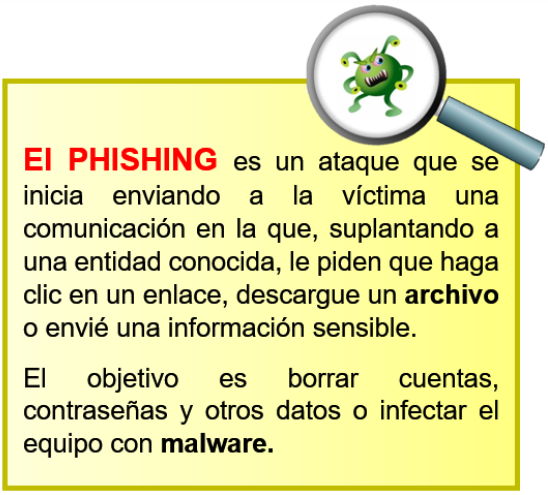


Figura 21. Definición de Phishing

Se puede presentar de dos formas:

1. Nosotros como empleados podemos recibir un email, que en realidad es fraude con el que intentarán robarnos los datos personales, es decir, seremos los «pescados»;

2. Nuestra página web puede ser atacada para suplantar a otra y enviar correos de Phishing con los que robar datos personales de clientes de la entidad suplantada, es decir seremos «la caña del pescador».

- **Como actúa el phisher**

1. El ciberdelincuente nos selecciona como la organización que va a suplantar.

2. Según el tipo de información que desea obtener, selecciona el medio a través del cual va a difundir su falso mensaje (el correo del Banco o el portal Bancario).

3. Por lo general el mensaje es alarmista y provocara en el usuario una reacción, que lo impulsa a hacer clic en un enlace o descargar y ejecutar un **fichero** adjunto.

4. Se redirige al usuario víctima a una página web falsa, que es similar a la legítima de la organización suplantada.

5. El usuario, confiado de que se encuentra en el sitio oficial, llena distintos formularios en la web maliciosa.

6. Finalmente, los datos capturados son almacenados en algún servidor remoto controlado por ciberdelincuentes y utilizados después para acciones fraudulentas como por ejemplo: suplantar la identidad de alguien, secuestro de cuentas de usuario, cometer delitos en su nombre, envío de spam, entre otros.

- **Como identifico un correo Phishing**

Los correos de Phishing tienen características comunes que ayudan a identificarlos, estas son:

1. Te incitan a tomar una decisión de manera urgente, con la recomendación de que se tendrá algún problema como el bloqueo de algún acceso, problema de seguridad, incluyen mensajes como “No ha finalizado correctamente su sesión, por favor, dar click en el siguiente enlace para hacerlo”, “Para contribuir a las políticas de seguridad, por favor cambia tus claves de acceso en el siguiente enlace”.

2. Se desconoce el remitente y el dominio no coincide con la empresa que supuestamente emite el correo, por ejemplo se recibe un correo del Portal del Banco de la Republica, pero el dominio no incluye el nombre del BANCO.

Figura 22. Ejemplo de Phishing 1

3. El contenido del mensaje tiene errores o incoherencias en la redacción o posee símbolos o caracteres extraños.

4. Poca personalización del mensaje, muchos de estos correos están dirigidos de manera general, sin incluir tu nombre, por ejemplo “Estimado señor”, como se muestra en la figura 23. Se debe tener en cuenta que muchos ciberdelincuentes utilizan tu nombre y hasta datos para hacer más confiable el engaño, de igual forma se debe tener cuidado.

5. Los archivos adjuntos al correo son por lo general son un fichero comprimido**. Zip** o un ejecutable**.exe** y pueden tener más de una extensión así: “nombredelfichero.doc.zip”, no hay que descargarlo ya que es alta la probabilidad de que se infecte nuestro equipo.


Notificacion
de Seguridad

Mundo Mujer
El Banco de la Comunidad

Apreciado Cliente,

Por procedimientos de seguridad, suspendimos de manera temporal el uso de sus productos y el acceso a los canales virtuales.

Lo invitamos a restablecer el acceso a todos nuestros canales, para ello debemos verificar la titularidad de usted como cliente.

Haga click en el link y comience el proceso de manera rapida, agil y segura. Asi de facil, sin necesidad de desplazarse a una oficina. Restablecer mi Cuenta <http://sneaker****.gr/https/>

Restablecer mi Cuenta

Diligencie la informacion solicitada, nuestro sistema verificara de manera inmediata y usted ingresara de manera normal a su cuenta, y de esta manera continua disfrutando de todos nuestros servicios nuevamente.

En Bancolombia a un Clic estamos innovando para que pueda disfrutar de mas tiempo libre, tener la oportunidad de contar con servicios agiles y simples, y estar para usted cuando, como y donde nos necesite.

Juan Diego Agudelo Ordonez
Gerencia Canales Digitales

Figura 23. Ejemplo de Phishing 2

- **¿Qué debo hacer en caso de ser víctima de Phishing?**

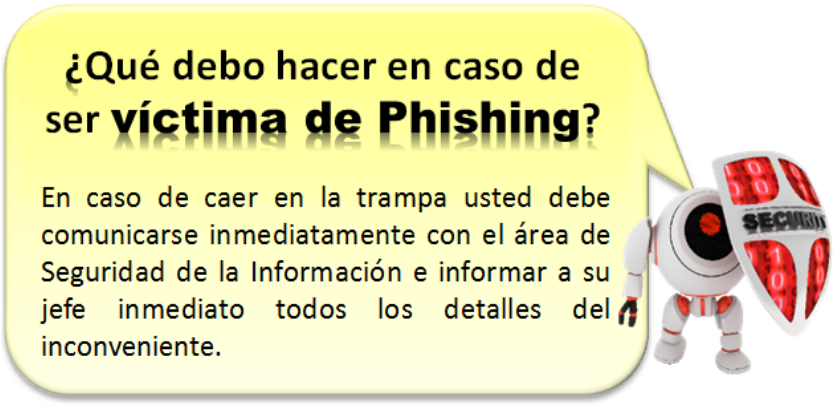


Figura 24. Acciones a tomar si es víctima de Phishing.

Figura 25. Consejos de Ciberseguridad

3.4 ESTRATEGIAS DE CAPACITACIÓN Y SENSIBILIZACIÓN

1. Salvapantallas en los ordenadores y televisores de la dirección general, que incluyan de manera breve frases de sensibilización en Seguridad de la información.

2. Distribución de objetos con mensajes relacionados a temas específicos. Por ejemplo, la distribución de cepillos de dientes asociados al mensaje del uso de la contraseña, en donde se hace una analogía del uso del cepillo de dientes con la utilización de las contraseñas: es de uso personal, no se presta a terceros y se debe cambiar frecuentemente.

3. Envió de mensajes o mailings a través de Correo electrónico de manera periódica, que refuercen las políticas o procedimientos de seguridad, como por ejemplo: el Manejo de Incidentes, Manejo de información confidencial, entre otros.

4. Realizar pruebas a los usuarios como forma de concienciación y sensibilización sobre los riesgos de Seguridad de la información.

Esta prueba consiste en un ataque dirigido enviado a los correos de los usuarios, con el cual se le convencerá de que descargue y abra un fichero adjunto infectado, el cual lo redireccionara a una página con un mensaje de sensibilización (ver anexo 2).

3.5 ALCANCE

El plan de capacitación y sensibilización en seguridad de la información para el primer semestre de 2018, está dirigido a los usuarios finales, administradores de plataformas, gerentes y personal interno con acceso a información.

Según datos del directorio activo del BMM, la dirección general del banco actualmente cuenta con **400** colaboradores activos.

4. EVALUACIÓN DEL PLAN DE CAPACITACIÓN Y SENSIBILIZACIÓN

La evaluación de las jornadas de capacitación se realizara a través de un examen presencial con las preguntas del Anexo 1: Banco de Preguntas y el Anexo 3. Evaluación de la Capacitación

5. CAMPAÑAS DE SENSIBILIZACIÓN

Las campañas de sensibilización contienen mailings relacionados con la seguridad de la información, los primeros para difundirse a través de correo electrónico a todos los funcionarios del banco incluyendo las agencias, o siguiendo alguna estrategia de divulgación. Estos Mailings se encuentran en el Anexo 4.

6. PLAN DE CAPACITACIÓN CONSOLIDADO

Responsables: Analistas y Especialista de Seguridad de la Información.
Requerimiento de recursos: Teniendo en cuenta que la duración de cada jornada de capacitación es de (1,6) horas, que el espacio físico de la capacitación será la sala de juntas del

BMM, la cual está dotada de todas las herramientas necesarias para la capacitación (video beam, tableros, marcadores, sonido), no es necesario la destinación de presupuesto para la ejecución del Plan de Capacitación y sensibilización.

Tabla 12. Plan de Capacitación y Sensibilización en Seguridad de la Información

PLAN DE CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN			
OBJETIVO DEL PLAN	**ACTIVIDAD**	**DETALLE**	**TIEMPO (SEMANAS)**
* Realizar campañas de sensibilización sobre seguridad de la información a través de mailings. * Incrementar los conocimientos sobre las Políticas de S.I establecidas en el BMM. * Reducir los riesgos de S.I asociados a la perdida de información producto de virus informático.	1. Elaboración de mailings.	Diseño, y revisión de mailings.	
	2. Difusión de mailings/ Políticas de Seguridad de la Información	1. Uso de contraseñas.	
		2. Uso del correo electrónico.	
		3. Buen uso de internet.	
		4. Seguridad para dispositivos USB	
		5. Uso y control de portátiles.	
		6. Escritorio y pantalla limpia.	
		7. Uso del servidor de archivos.	
	3. Difusión de mailings/ vulnerabilidades de Seguridad de la información	8. Ciberseguridad.	
		9. Malware	
		10. Rasomware	
		11. Phishing	
	4. Elaboración y difusión de Salvapantallas	Salvapantallas de Sensibilización (políticas DNC)	
	5. Capacitación de colaboradores	30 jornadas de capacitación (6 semanales).	
	6. Campaña sensibilización ciberseguridad	Simulación de malware, mediante correo dirigido.	
	7. Elaboración de informe final	Informe de los resultados de la capacitación.	

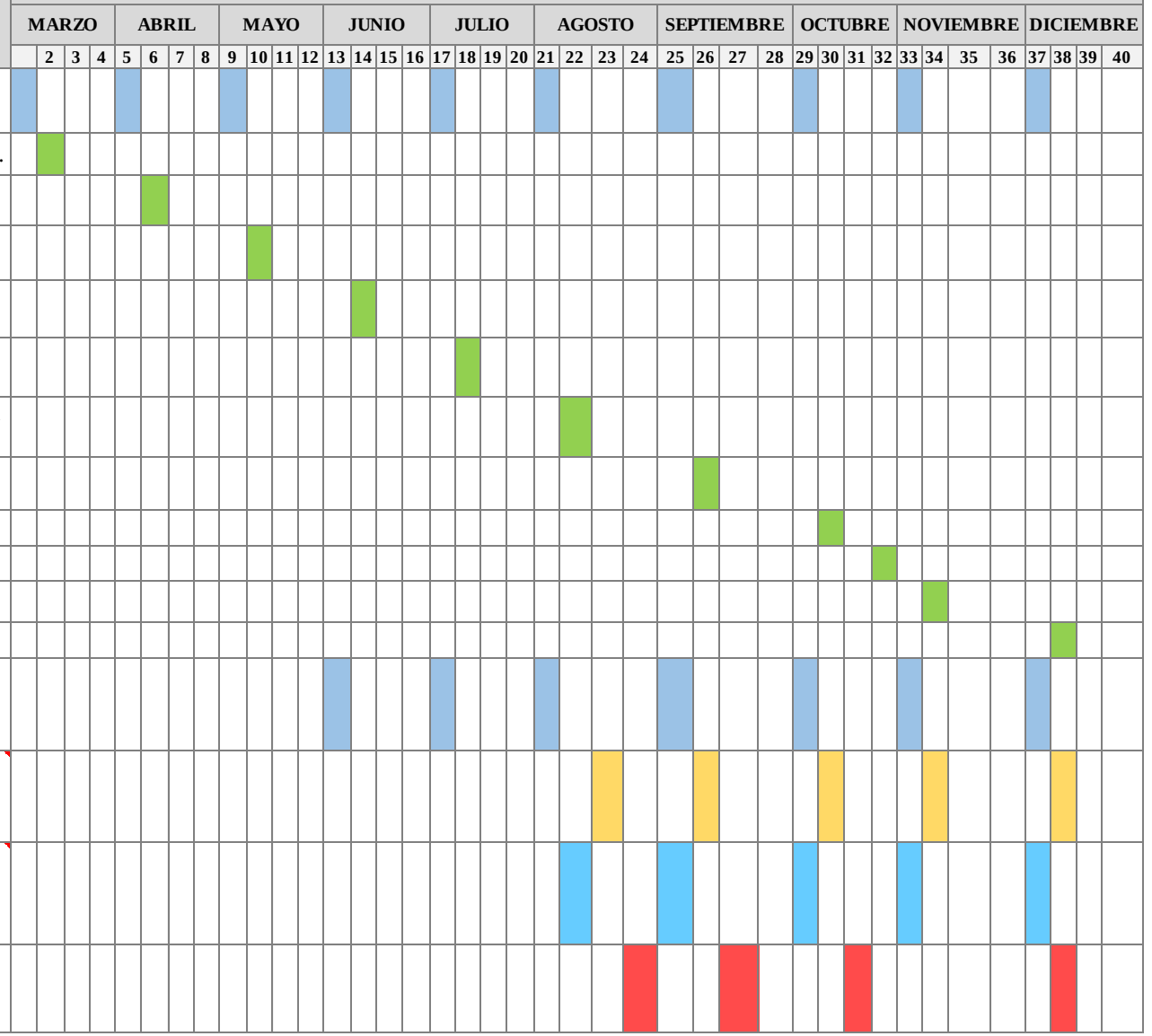


Tabla 13. Avance del Plan a 31 de Julio de 2018.

AVANCE DEL PLAN - JULIO 2018						
OBJETIVO	**ACTIVIDAD**	**INDICADOR / ACTIVIDAD**	**DESCRIPCIÓN**	**VALOR**		**RESPONSABLE**
* Realizar campañas de sensibilización sobre seguridad de la información a través de mailings.	1. Elaboración de mailings.	N° mailings revisados ---------- X 100 N° mailings elaborados	Elaborar 2 mailings la 1er semana de cada mes, en total 20. Según el DNC 10 Campañas en total.	(5/10)	50%	Pasante y Gerente Riesgos NF
	2. Difusión de mailings/ Políticas S.I	N° mailings enviados ---------- X 100 N° mailings programados	10 mailings según el DNC.	(5/10)	50%	Gerente de Riesgos No Financieros
	3. Difusión de mailings/ Vulnerabilidades S.I					
	4. Elaboración de Salvapantallas	N° Salvapantallas ---------- X 100 N° Políticas del DNC	A fecha del 31 de Julio se han elborarón 3 salvapantallas	(3/7)	43%	Pasante Universitario
* Incrementar los conocimientos sobre las Políticas de S.I establecidas en el BMM. * Reducir los riesgos de S.I asociados a la perdida de información producto de virus informático.	5. Capacitación de colaboradores	Total personas capacitadas ---------- X 100 Total personas a capacitar	Total de colaboradores 400, capacidad de sala de juntas de 15 personas, (26) se programan 30 capacitaciones teniendo en cuenta los colaboradores que no asistan inicialmente.	(X/400)	0%	Analistas y Especialista de S.I
	6. Campaña sensibilización ciberseguridad- ataque simulado	Total correos enviados ---------- X 100 Total personas a capacitar	Se envía antes de cada capacitación presencial, según el listado de personas.	(X/400)	0%	Especialista de Seguridad de la Información.
	7. Elaboración de informe final	Documento final	Elaboración de un informe final con el cumplimiento del Plan, las conclusiones y sugerencias.			Analista de Seguridad de la Información

5. CONCLUSIONES Y SUGERENCIAS

1. El Plan de Capacitación y Sensibilización en Seguridad de la información es una herramienta para mitigar los riesgos asociados a la seguridad de la información, ya que permite mejorar las competencias de los colaboradores frente a las políticas y vulnerabilidades en Seguridad de la Información.

2. Los principales riesgos que se mitigan con el Plan de capacitación y sensibilización en Seguridad de la información son: fraude interno, fugas de información y pérdidas de información por virus informático.

3. Las principales políticas de seguridad de la información establecidas desde el área de seguridad de la información son siete: uso de contraseñas, uso del correo institucional, buen uso de internet, seguridad para los dispositivos USB, uso y control de portátiles, escritorio y pantalla limpia y uso del servidor de archivos.

4. Las necesidades de capacitación y sensibilización del Banco Mundo Mujer son principalmente dos: Conocimiento de las Políticas de S.I y La identificación de vulnerabilidades de los sistemas de información por parte de los colaboradores.

5. La puesta en marcha del Plan de Capacitación y Sensibilización en Seguridad de la información permite que los colaboradores conozcan y se apropien de las principales políticas de seguridad de la información.

6. Se recomienda que los mailings que se elaboran sean revisados por más de una persona, que solo el Gerente de Riesgo no financieros, con el fin de realizar más campañas y cumplir los objetivos del Plan.

REFERENCIAS BIBLIOGRÁFICAS

Chiavenato, Idalberto (2007). *Administración de Recursos Humanos, El capital Humano de las Organizaciones,* McGraw-Hill, México, 8tava Edición, pp. 384-413.

Grados Espinosa, Jaime A. (2009). *Capacitación y desarrollo de personal*, Trillas, 4ta Edición, México. pp. 201-277.

William B. Werther y Keith Davis (2008), *Administración de Recursos Humanos, El capital Humano de las empresas,* McGraw-Hill, México, 6ta Edición.

Silíceo Aguilar, Alfonso (2004) *Capacitación y desarrollo de Personal*, EDITORIAL LIMUSA, S.A., México, 4ta Edición.

Gómez, Marcelo M (2006) *Introducción a la Metodología de la Investigación Científica*, Editorial Brujas, Argentina, 1ra ED.

ESET Latinoamérica, *Eset Security Report Latinoamérica 2012 / Eset Security Report Latinoamérica 2017*

Reza Trosino, Jesús Carlos, (2006) *Nuevo diagnóstico de necesidades de capacitación y aprendizaje en las organizaciones*, EDT. Panorama, 1ra edición, México.

Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información, Guía N° 14 MINTIC.

Ortegón Edgar, Pacheco Francisco, Roura Horacio (2005). *Metodología general de identificación, preparación, y evaluación de proyectos de inversión pública,* Instituto o Latinoamericano y del Caribe de Planificación Económica y Social (ILPES), ISSN electrónico 1680-8878, Santiago de Chile, pp. 10-18.

Diego Gómez Cáceres, Jesús Miguel López Zaballos (2002) *Riesgos financieros y operaciones internacionales,* Editorial ESIC, ISBN: 84-7356-326-3, Madrid.

© Banco Interamericano de Desarrollo, 1999 ISBN: 1-886938-47-4, Gestión de riesgos financieros: un enfoque práctico para países latinoamericanos.

Consejo Federal de Inversiones, *Guía para la Elaboración de Planes de Capacitación* , Instituto Provincial de la Administración Pública IPAP, (Marzo 2015), Buenos Aires Argentina.

LECHUGA S. Efraín (2006): *Estrategias para la optimización de los recursos humanos*, Grupo Editorial ISEF, 1a. ed., 3a. reimpr., México.

Norma Técnica Colombiana ISO 27001: 2013, Sistema de Gestión de Seguridad de la Información.

Norma Técnica Colombiana ISO 31000: Gestión del Riesgo, Principios y directrices.

PT 007: (2018), Políticas de Seguridad de la Información del Banco Mundo Mujer, Versión 002.

ANEXOS

1. Banco de Preguntas

Preguntas con única respuesta – (Resaltada se encuentra la respuesta verdadera)

1. Mantener documentos tales como pagares, contratos e información de clientes bajo custodia hace parte de la política de:
   a. Uso de Internet
   b. Uso de correo
   c. Escritorio limpio
   d. Uso de contraseñas

2. Cuáles son los criterios de seguridad de la información:
   a. Integridad, Cumplimiento y Confidencialidad
   b. Integridad, Confidencialidad, Disponibilidad.
   c. Efectividad, Integridad y Disponibilidad
   d. Ninguna de las anteriores

3. Teniendo en cuenta la diferencia entre Ciberseguridad, Seguridad de la Información y Seguridad Informática, rellene los espacios con la respuesta correcta:

A. _Ciberseguridad___ busca proteger la información digital en los sistemas interconectados (Ciberseguridad).
B. _Seguridad Informática___ atiende a la protección de las instalaciones informáticas y de la información de medios digitales.
C. __Seguridad de la Información___ integra toda la información independientemente del medio en el cual este.

4. Relacione los siguientes conceptos:

1. MALWARE	(**2**) Permite que un ciberdelincuente secuestre nuestro equipo de manera remota y encripte nuestra información.
2. RASOWARE	(**1**) Cualquier software malicioso que tiene como objetivo infiltrarse y causar daño en el quipo o Sistema de información.

3. PHISHING	(**3**) Engaño en el cual un ciberdelincuente suplanta la identidad de una persona o empresa, utilizando el correo electrónico.

5. Marque Falso (F) o Verdadero (V) según cada afirmación:

La contraseña deberá ser actualizada cada 15 días.	F
Los Vicepresidentes y Gerentes serán los únicos autorizados para el uso de medios de almacenamiento masivo USB en la Dirección General	V
En el servidor de archivos puede ser almacenada información personal tales como documentos, archivos de imagen, videos, y ejecutables.	F
Usted puede utilizar el correo institucional para asuntos de índole personal tales como suscripciones, recepción de información de portales de noticias y entretenimiento.	F

6. Fernando Ortega tiene una cuenta de ahorros con el banco Mundo Mujer. Este dato se clasifica como:

a. Un buen dato.
b. Un dato semiprivado.
c. Un dato sensible.
d. Un dato que solo le interesa al banco.

7. El dato sensible es:

a. Aquel que se puede obtener sin reserva alguna.
b. Datos que se comparten en las redes sociales.
c. Que afecta la intimidad y su uso indebido puede generar discriminación.
d. Los datos que aparecen en el carnet institucional

8. ¿Cuál es el objetivo del plan de continuidad del negocio?

a. Brindarle comodidad a los clientes mientras que se restablece el orden en la entidad.
b. Evitar que la entidad interrumpa sus operaciones.
c. Dejar que todo vuelva a su completa normalidad.
d. No permitir que los clientes abandonen la entidad.

9. Quién debe mantener protegida la información de nuestra entidad:

a. La Dirección, el Comité de Riesgos y Seguridad de la Información
b. La Vicepresidencia de Riesgos, la Junta Directiva y el Comité de Riesgos.
c. Todos los funcionarios de la entidad

d. Los funcionarios que manejan información de clientes.

10. Un activo de información es aquel que contiene información valiosa y necesaria para la operación del Banco, según este concepto relacione la definición de los siguientes activos de información.

1. Intangibles	3. Calificación, competencia y experiencia.
2. Electrónicos	1. Ideas, conocimiento y conversaciones.
3. Personas	5. pueden ser computaciones y de comunicaciones.
4. Físicos	4. Documentos impresos, manuscritos y hardware.
5. Servicios	2. Bases de datos, archivos, registros de auditoria, aplicativos.

2. Ataque dirigido

Esta prueba está basada en el envío de un correo electrónico con un fichero infectado, el cual, al ser abierto dirige al usuario a un portal Web, en el cual se le advierte de los riesgos por lo que acaba de hacer. El correo debe ser enviado masivamente, con un asunto claro y confiable, el mensaje de sensibilización es el siguiente:

ATAQUE SIMULADO

Una situación como esta podría haberte pasado con un correo de un hacker o algún colaborador interno, pero esta es una **prueba controlada**. Esta vez te has librado, pero ha sido fácil engañarte, ¿verdad?

Recuerda que abrir o ejecutar un archivo del cual desconoces su procedencia, puede generar la infección de tu equipo.

En este caso solo deseábamos llevarte a esta misma página Web. Sin embargo, ¿Que podría haber sucedido si este fichero hubiese sido un malware real?

Estos son algunos ejemplos de lo que pudo pasar:

- El fichero puede ser un troyano en el que un ciberdelincuente acceda a tu equipo y, desde él, al resto de equipos del Banco.
- El fichero puede ser un gusano que infecta tu equipo, y se propaga por toda la red de la empresa.

- El fichero puede ser un virus y puede realizar acciones dañinas sobre tu equipo, como borrar o dañar archivos.

Debes ser consciente de las vulnerabilidades y peligros inminentes en los sistemas de información y recuerda que el BMM cuenta con unas Políticas de Seguridad de la Información establecidas. Es necesario que las conozcas y apropies de ellas. **¡La seguridad de la información es tarea de todos!**

Una vez finalizada la prueba, se debe solicitar a los usuarios la eliminación del fichero descargado.

3. Formato de evaluación de capacitación

Mundo Mujer El Banco de la Comunidad	**Evaluación del Impacto de la Capacitación en Seguridad de la Información**	**Código**	FM 01
		Página	72 de 1

Fecha: _____

Nombre: _____ **Cargo:**_____ **Área:**_____

Las preguntas adjuntas le permiten expresar su opinión con relación a los conocimientos adquiridos en esta capitación.

Lea cada punto cuidadosamente y responda con toda sinceridad ya que esto permite obtener la información adecuada para mejorar futuras capacitaciones o cursos de formación.

Marque con una X la opción que crea conveniente.

CUESTIONARIO

Evalué de 1 a 5 los siguientes aspectos, teniendo en cuenta que:

1. Muy malo
2. Malo
3. Regular
4. Bueno
5. muy bueno

ASPECTO A EVALUAR	1	2	3	4	5
1. Eficacia de la metodología					
2. Dominio del tema por parte de los capacitadores					
3. Pertinencia del horario					
4. Pertinencia del lugar					

1. Antes de esta capacitación, mi nivel de conocimientos o competencias para el objetivo de este curso era.			
Malo	**Regular**	**Bueno**	**Excelente**
2. Después de esta capacitación mi nivel de conocimientos o competencias para el objetivo de este curso era.			
Malo	**Regular**	**Bueno**	**Excelente**
3. Estime que porcentaje de lo aprendido en esta capacitación que podrá aplicar en su trabajo.			
25%	**50%**	**75%**	**100%**
4. Para mejorar futuras capacitaciones indique los temas a los cuales se les podría			
Adicionar	**Dar Más énfasis**	**Dar Menos énfasis**	**Suprimir**

4. Material de sensibilización

Salvapantallas y mailings


HORA DE MARCHARSE = HORA DE GUARDAR LA INFORMACIÓN
VICEPRESIDENCIA DE RIESGOS
Seguridad de la Información
Mundo Mujer
El Banco de la Comunidad


¿Tu contraseña es 1234?
¡M3j0r c4m8i4L4 P0R 0TR4!
****
VICEPRESIDENCIA DE RIESGOS
Seguridad de la Información
Mundo Mujer
El Banco de la Comunidad


4 RESTRICCIONES PARA EL USO DEL SERVICIO DE INTERNET
OneDrive
Como parte de las políticas de Seguridad de la información (PT 007), se han establecido unas restricciones sobre el uso de internet, hoy recordaremos 4 de las mas importantes, las cuales ayudan a evitar los riesgos de pérdida de integridad, confidencialidad, disponibilidad o fuga de la información
1. ¿Puedo descargar alguna aplicación?
Recuerde que no esta autorizada La descarga de software, programas o aplicaciones de cualquier tipo.
2. Búsqueda de Contenido Multimedia
No esta permitido el uso de aplicaciones de búsqueda para la obtención de archivos comerciales, música o videos con derechos reservados.
3. Almacenamiento en la NUBE
Se prohíbe, el uso de portales y/o aplicaciones para almacenar información en la nube como Dropbox, Skydrive, Google Drive, icloud, entre otros.
Google Drive
4. Sobre el Correo Electrónico
No olvide, que esta restringido el acceso a los portales del correo electrónico personal como Hotmail, Gmail, Yahoo!, entre otros.
VICEPRESIDENCIA DE RIESGOS
Seguridad de la Información
Mundo Mujer
El Banco de la Comunidad

TIPS PARA USO DE CONTRASEÑAS

TEN CUIDADO

El préstamo de tu contraseña con o sin intensión, te hace responsable de las consecuencias a las que conlleven las acciones que se realicen con tus credenciales (usuario y contraseña) durante ese tiempo. **¡No asumas responsabilidades por otras personas!**

AYUDA A EVITAR EL FRAUDE

Nunca prestes tu usuario y contraseña, ya que son de uso personal e intransferible, por ningún motivo debe ser suministrada, compartida, escrita o divulgada través de correo electrónico u otro medio, a ningún funcionario o personal externo del banco.

RECUERDA...

Puedes cambiar la contraseña en cualquier momento o en alguna de las siguientes situaciones:

- Crees que alguien la conoce.
- Te la han robado/copiado.
- No la recuerdas.
- Dejaste tu sesión iniciada.
- Tu contraseña es fácil de descifrar.

¿CÓMO DEBE SER MI CONTRASEÑA?

Como parte de las políticas de seguridad de la información las contraseñas en los sistemas de información deberán cumplir con las siguientes características:

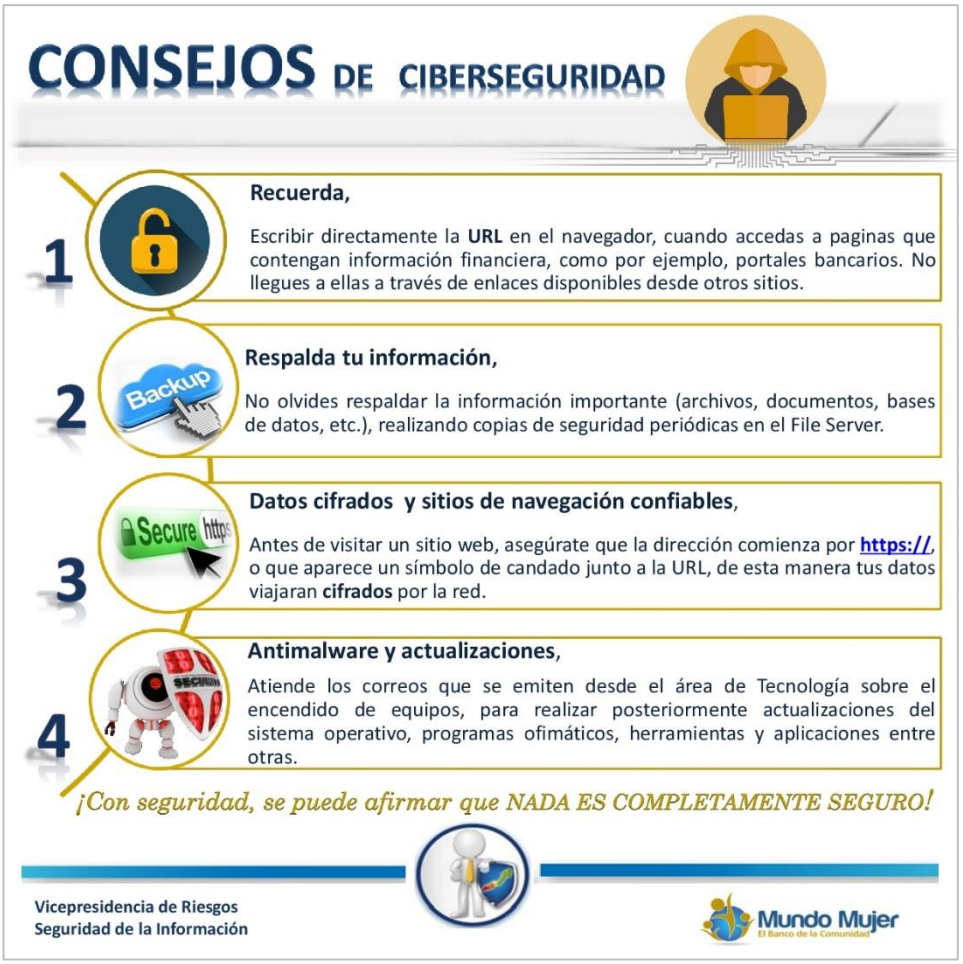
- Mínimo 8 y máximo 10 caracteres.
- Utilizar números, letras y símbolos especiales.
- No utilizar nombre de usuario asociado.
- No repetir los mismos caracteres en la misma contraseña ej: “111222”.
- No utilizar secuencias básicas de teclado, como “qwert” “abcde” “1234” o “9876”.

“LAS CONTRASEÑAS SON LA PRIMERA LÍNEA DE DEFENSA EN LA PROTECCIÓN DE NUESTRA IDENTIDAD VIRTUAL”

VICEPRESIDENCIA DE RIESGOS
SEGURIDAD DE LA INFORMACIÓN

Mundo Mujer
El Banco de la Comunidad


6 CONSEJOS DE ESCRITORIO LIMPIO
¡TU PUESTO DE TRABAJO ES CLAVE PARA LA SEGURIDAD DE LA INFORMACIÓN!
1
CONFIDENCIAL
Guarda tu información física en un lugar adecuado, tu escritorio debe permanecer limpio de documentos importantes como: Información de clientes, contratos, recibos, entre otros.
¡Así contribuyes a proteger la confidencialidad de la información!
2
Asegúrate de no dejar documentos olvidados en las impresoras, estos pueden contener información sensible de nuestros clientes y la operación del Banco
¡Tú y la información son nuestros activos mas valiosos!
3
Recuerda que la documentación que no utilices, debe estar guardada correctamente, especialmente cuando dejas tu puesto de trabajo y al finalizar la jornada laboral.
¡Eres responsable de la adecuada disponibilidad de la información!
4
Destruye la documentación física de forma segura, revisando que lo desechado NO contenga ningún tipo de información sensible (firmas, datos de clientes, entre otros).
¡De esta manera proteges la integridad y confidencialidad de la información!
5
DANGER
No olvides, que esta prohibido imprimir reutilizando papel que contenga información de nuestros clientes y la operación del Banco.
¡La Seguridad de la información, es tarea de todos!
6
No utilices el escritorio de tu PC como carpeta temporal para almacenar o dejar trabajos recientes o pendientes, el escritorio de tu PC también debe permanecer limpio
¡Ayuda a evitar cualquier fuga de información!
VICEPRESIDENCIA DE RIESGOS
Seguridad de la Información
Mundo Mujer
El Banco de la Comunidad


CONSEJOS DE CIBERSEGURIDAD
1
Recuerda,
Escribir directamente la URL en el navegador, cuando accedas a paginas que contengan información financiera, como por ejemplo, portales bancarios. No llegues a ellas a través de enlaces disponibles desde otros sitios.
2
Backup
Respalda tu información,
No olvides respaldar la información importante (archivos, documentos, bases de datos, etc.), realizando copias de seguridad periódicas en el File Server.
3
Secure https
Datos cifrados y sitios de navegación confiables,
Antes de visitar un sitio web, asegúrate que la dirección comienza por https://, o que aparece un símbolo de candado junto a la URL, de esta manera tus datos viajaran cifrados por la red.
4
Antimalware y actualizaciones,
Atiende los correos que se emiten desde el área de Tecnología sobre el encendido de equipos, para realizar posteriormente actualizaciones del sistema operativo, programas ofimáticos, herramientas y aplicaciones entre otras.
¡Con seguridad, se puede afirmar que NADA ES COMPLETAMENTE SEGURO!
Vicepresidencia de Riesgos
Seguridad de la Información
Mundo Mujer
El Banco de la Comunidad

ASIGNACIÓN Y USO DE COMPUTADORES PORTÁTILES

Recordemos algunos consejos y recomendaciones sobre la asignación y uso de computadores portátiles, establecidos en las **Políticas de seguridad de la Información** (PT007).

1

¿QUIÉNES TIENEN UN COMPUTADOR PORTÁTIL?

Recuerda que los computadores portátiles, están asignados en primera instancia a: Presidencia, Vicepresidencia, Gerentes, Jefes de áreas y Áreas de control.

2

ASIGNACIÓN TEMPORAL

Recuerde que en caso de que un funcionario tenga que realizar labores fuera de las instalaciones, a través del área de soporte de TI se le asignará un computador portátil temporal.

VISITANTES Y/O TERCEROS

- Si realizan actividades de corto tiempo (< 3 días), podrán hacer uso de su computador portátil personal, bajo supervisión de funcionarios del banco.
- Si tienen vinculo comercial, les será signado un computador portátil, el cual cumplirá las políticas y tendrá todos los controles que ha establecido el banco para proteger la información

3

¿PUEDO PRESTAR MI COMPUTADOR PORTÁTIL?

Ten en cuenta que los computadores portátiles asignados, tienen carácter intransferible y son responsabilidad del personal respectivo, por tanto **NO deben ser prestados.**

¡RIESGOS!

Debido a las características de este tipo de equipos, se pueden presentar más vulnerabilidades de Seguridad de la información, tales como: Fuga de información, Fraudes, sustracción o pérdida de información, entre otros; además, se debe considerar que estos equipos son más susceptibles a robo o pérdida.

RECUERDA...

Si necesitas realizar una presentación, cada sala de reunión o de gerencia cuenta con un computador portátil con acceso al File Server, en el cual puedes proyectar las presentaciones; ten en cuenta, que debes llegar como mínimo con 15 minutos de anticipación para conectar tu usuario al file server y realizar las respectivas pruebas

¡LA SEGURIDAD DE LA INFORMACIÓN ES RESPONSABILIDAD DE TODOS!

VICEPRESIDENCIA DE RIESGOS
Seguridad de la Información

Mundo Mujer
El Banco de la Comunidad


¿PUEDO INTERCAMBIAR Y ALMACENAR INFORMACIÓN EN LA NUBE?
box
Dropbox
OneDrive
iCloud
Google Drive
¡RESTRINGIDO!
Tenga en cuenta que en las Políticas de Seguridad de la Información PT 007, literal 5.1.4, se prohíbe el uso de portales y/o aplicaciones para almacenar información en la nube como por ejemplo: Dropbox, Skydrive, Google Drive, icloud, entre otros.
¿POR QUÉ?
Es nuestro deber proteger la información de nuestros clientes y las operaciones del banco, evitando los riesgos de seguridad de la información asociados a los servicios gratuitos de almacenamiento en la nube, tales como: fugas de información, plagio de propiedad intelectual, fraudes y/o suplantaciones.
Crear mensaje
Cifrarlo
Envío seguro
¿CÓMO PUEDO INTERCAMBIAR INFORMACIÓN DE FORMA SEGURA?
Recuerde que el banco cuenta con las siguientes opciones para enviar y/o recibir información a nivel interno y externo con proveedores o terceros:
• Correo institucional con adjuntos cifrados o contraseñas.
• SFTP
• File Server o servidor de archivos, utilizando carpetas comprimidas con clave .
• Creación e intercambio de llaves asimétricas entre el banco y el proveedor.
¡¡RECUERDE ESTAS POLÍTICAS DE SEGURIDAD, Y EXIJA A LOS TERCEROS CON LOS QUE TIENE RELACIÓN UTILIZAR LAS HERRAMIENTAS QUE EL BANCO HA DESTINADO PARA TAL FIN!!
VICEPRESIDENCIA DE RIESGOS
Seguridad de la Información
Mundo Mujer


¡CIERRA TU SESIÓN!
Hola, hoy recordaremos la Política de Seguridad de la Información sobre sesión abierta.
1
Debes cerrar tu sesión cada vez que te ausentes de tu puesto de trabajo.
Aunque te encuentres cerca, en ningún momento debes dejar tu sesión desatendida.
2
Recuerda que puedes reportar las sesiones abiertas enviando un correo desde el equipo de la sesión abierta a infoseguridad@bmm.com.co con copia al jefe inmediato incluyendo en el asunto: Sesión Abierta
3
Tú jefe de área tiene la responsabilidad de diseñar sanciones de tipo educativo, como por ejemplo:
✓ Multa $.
✓ Elaborar una presentación o cartelera sobre Seguridad de la Información para tus compañeros.
✓ Compartir un pasabocas con tus compañeros.
Jefe, !Vengo a cancelar la multa!
Perfecto, recuerda cerrar siempre tu sesión al levantarte de tu puesto.
¡Oye!, ¿Cerraste tu sesión?
No, espera un momento.
¡sesión abierta, sesión abierta!
"ES NUESTRA RESPONSABILIDAD PROTEGER LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN"
VICEPRESIDENCIA DE RIESGOS
Seguridad de la Información
Mundo Mujer

RECORDEMOS ALGUNAS POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN

1 ¡BLOQUEA TU SESIÓN!

Recuerda que debes bloquear la sesión, cada vez que te ausentes de tu puesto de trabajo y que en ningún momento debes dejar tu sesión desatendida, aunque te encuentres cerca.

2 PANTALLA LIMPIA

La pantalla de tu computador debe contener exclusivamente los iconos definidos por el área de TI.

¡La información valiosa no debe estar a primera vista de terceros!

3 CONFIDENCIALIDAD DE LA INFORMACIÓN

El escritorio de tu computador debe mantenerse sin accesos directos no autorizados y sin documentos guardados en él.

AYUDA A EVITAR RIESGOS

- *Suplantación de identidad.*
- *Fuga de información, por acceso no autorizados a los repositorios de información.*
- *Fraude interno, sustracción de información confidencial de la entidad.*
- *Accesos no autorizados a información confidencial y repositorios como el servidor de archivos.*
- *Transferencias y cualquier modificación de información en los sistemas de información del BMM.*

4 ESCRITORIO LIMPIO

Debes mantener tu escritorio limpio de documentos importantes, tales como: Información de clientes, contratos, recibos, entre otros.

5 DISPONIBILIDAD DE LA INFORMACIÓN

Debes mantener la información física y digital protegida o no disponible en los tiempos que no te encuentres en tu puesto de trabajo.

VICEPRESIDENCIA DE RIESGOS
Seguridad de la Información

Mundo Mujer
El Banco de la Comunidad

FOLLETO N° 1

SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Ciertos individuos considerados como Intrusos, atacantes o Hackers, continuamente están tratando de obtener acceso en forma ilícita a los Sistemas de Información de las organizaciones y para esto utilizan diferentes tipos de ataques.

Las compañías invierten gran cantidad de tiempo y presupuesto en "prevenir" estos ataques; sin embargo, la mayoría de los métodos para obtener acceso a la información NO requieren un elevado conocimiento técnico inicial.

¿Por qué?

Debido a los errores que cometemos como usuarios, algunos son:

1. Compartir el usuario o la contraseña
2. Abrir archivos adjuntos de correo de origen desconocido
3. Utilizar el correo de la organización para enviar "SPAM"
4. Instalar software no autorizado.
5. No colocar en las carpetas del File server la información de trabajo.
6. Navegar en sitios "peligrosos".

ALGUNOS CASOS REALES

- Organismos de Seguridad investigan a un empleado que envió un mensaje anónimo amenazando al presidente de la compañía.
- Empleado captura 500 contraseñas de los usuarios de la compañía.
- El grupo financiero pierde información de 1 año por no realizar Backup a la información.
- Despiden empleado por usar los recursos tecnológicos de la compañía para realizar negocios personales.

¿Qué debo hacer?

PRINCIPIOS FUNDAMENTALES DE LA SEGURIDAD DE LA INFORMACIÓN

Garantizar que la información no está disponible o divulgada a terceros no autorizados.

Mantener intacta y en buen estado los activos de información de la organización.

Mantener disponible y accesible la Información a los usuarios autorizados.

RECOMENDACIONES

- ✓ Recuerda que debes bloquear la sesión, cada vez que te ausentes de tu puesto de trabajo.
- ✓ El escritorio de tu computador debe mantenerse sin accesos directos no autorizados.
- ✓ Debes mantener tu escritorio limpio de documentos importantes, tales como: Información de clientes, contratos, recibos, entre otros.
- ✓ Debes utilizar contraseñas fuertes y cambiarlas frecuentemente.

VICEPRESIDENCIA DE RIESGOS
Seguridad de la Información

5. Evidencias

FECHA: 17-07-2018
NOMBRE DEL EXPERTO: Victoria Martinez.
CARGO: Analista Riesgo Operativo BMM. /Riesgos

PREGUNTA:

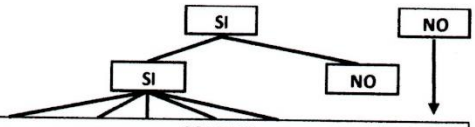
Teniendo en cuenta la estructuración de un plan de capacitación y sensibilización para reducir los riesgos de seguridad de la información ¿Cómo incide incluir las siguientes necesidades de capacitación en este plan?

OPINIÓN:

R (Rojo) No incide
r (rosado) Incide muy poco
A (Amarillo) Neutro
v (verde claro) Incide algo
V (Verde oscuro) Incide mucho
B (Blanco) No sabe
(Negro) No responde

¿Desea usted responder?

¿En caso afirmativo tiene usted alguna opinión al respeto?
¿Cuál?



ITEM: NECESIDAD DE CAPACITACIÓN	COLORES						
	V	v	A	r	R	B	N
1. Conocimiento de los aspectos básicos de seguridad de la información.			X				
2. Identificación de las principales vulnerabilidades de Seguridad de la información	X						
3. Manejo de Información Confidencial.			X				
4. Conocimiento de las Políticas de Seguridad de la Información.	X						
5. Gestión de la información		X					

FECHA: 17 Julio 2018
NOMBRE DEL EXPERTO: Marcela Solano
CARGO: Analista Seguridad de la Informa

PREGUNTA:

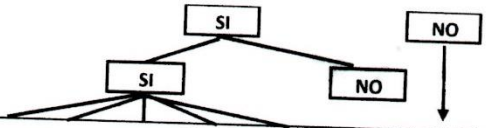
Teniendo en cuenta la estructuración de un plan de capacitación y sensibilización para reducir los riesgos de seguridad de la información ¿Cómo incide incluir las siguientes necesidades de capacitación en este plan?

OPINIÓN:

R (Rojo) No incide
r (rosado) Incide muy poco
A (Amarillo) Neutro
v (verde claro) Incide algo
V (Verde oscuro) Incide mucho
B (Blanco) No sabe
(Negro) No responde

¿Desea usted responder?

¿En caso afirmativo tiene usted alguna opinión al respeto?
¿Cuál?



ITEM: NECESIDAD DE CAPACITACIÓN	COLORES						
	V	v	A	r	R	B	N
1. Conocimiento de los aspectos básicos de seguridad de la información.		X					
2. Identificación de las principales vulnerabilidades de Seguridad de la información		X					
3. Manejo de Información Confidencial.				X			
4. Conocimiento de las Políticas de Seguridad de la Información.	X						
5. Gestión de la información		X					

FECHA: 18 - Julio - 2018
NOMBRE DEL EXPERTO: CARLOS RODALLEGA.
CARGO:
ESP. SEG. INFORMACIÓN.

PREGUNTA:

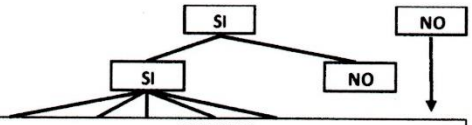
Teniendo en cuenta la estructuración de un plan de capacitación y sensibilización para reducir los riesgos de seguridad de la información ¿Cómo incide incluir las siguientes necesidades de capacitación en este plan?

OPINIÓN:

R (Rojo) No incide
r (rosado) Incide muy poco
A (Amarillo) Neutro
v (verde claro) Incide algo
V (Verde oscuro) Incide mucho
B (Blanco) No sabe
(Negro) No responde

¿Desea usted responder?

¿En caso afirmativo tiene usted alguna opinión al respeto?
¿Cuál?



ITEM: NECESIDAD DE CAPACITACIÓN	COLORES						
	V	v	A	r	R	B	N
1. Conocimiento de los aspectos básicos de seguridad de la información.	X						
2. Identificación de las principales vulnerabilidades de Seguridad de la información	X						
3. Manejo de Información Confidencial.		X					
4. Conocimiento de las Políticas de Seguridad de la Información.	X						
5. Gestión de la información	X						

FECHA: 19 julio de 2018
NOMBRE DEL EXPERTO: Juan Pablo Rodriguez C.
CARGO:
Gerente Riesgos No Financieros
PREGUNTA:

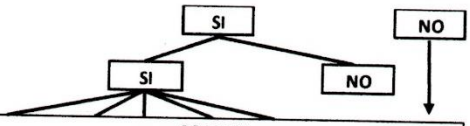
Teniendo en cuenta la estructuración de un plan de capacitación y sensibilización para reducir los riesgos de seguridad de la información ¿Cómo incide incluir las siguientes necesidades de capacitación en este plan?

OPINIÓN:

R (Rojo) No incide
r (rosado) Incide muy poco
A (Amarillo) Neutro
v (verde claro) Incide algo
V (Verde oscuro) Incide mucho
B (Blanco) No sabe
(Negro) No responde

¿Desea usted responder?

¿En caso afirmativo tiene usted alguna opinión al respeto?
¿Cuál?



ITEM: NECESIDAD DE CAPACITACIÓN	COLORES						
	V	v	A	r	R	B	N
1. Conocimiento de los aspectos básicos de seguridad de la información.	X						
2. Identificación de las principales vulnerabilidades de Seguridad de la información	X						
3. Manejo de Información Confidencial.	X						
4. Conocimiento de las Políticas de Seguridad de la	X						