Desarrollo de una guía de ciberseguridad para una pyme, basada en el nuevo framework NIST

Máster en Seguridad Informática UPC-VIU
Curso académico 2017 - 2018

Alumno/a:
Mainas Alessandro
D.N.I: YB1300749

Director de TFM:
José Elviro Blanco Vega

Convocatoria:
11-17 Febrero 2019

Fecha de defensa:
25 Febrero - 1 Marzo 2019

Resumen

El trabajo consiste en el desarrollo de una guía para la instalación de un cybersecurity framework para pequeñas y medias empresas. Estas empresas tienen pocos recursos, pero se ven involucradas más y más en el mundo de las CAMS (Cloud, Analytics, Mobile and Social Applications) y necesitan protegerse para ser competitivas.
El objetivo principal es obtener una guía orientada a la gestión del riesgo, que permita proporcionar soluciones eficaces a casos reales y hacer frente a las amenazas modernas. Para este motivo la guía está basada en el nuevo Cybersecurity Framework de NIST, el cual recolecta la mayoría de los estándares en controles de seguridad orientados a la gestión de riesgos. El Framework permaneciendo tecnológicamente neutro, permite la libre implementación de dichos controles.
La guía ha sido centrada en cuatro macrobjetivos que tocan cada uno de los puntos del Framework: Identify, Protect, Detect, Respond y Recover.
A través de estos objetivos, se quieren proporcionar soluciones ad hoc para pequeñas y medianas empresas. En particular, se quiere lograr una alineación y un equilibrio entre las medidas de seguridad y las necesidades del negocio, administrando los riesgos para reducir su posible impacto. Tratar de concienciar dinámicamente las áreas de la empresa creando programas distintos para cada una de ellas, lo que resultaría generar mayor interés e implicación del empleado en el programa de concienciación, aumentando la eficacia y eficiencia del proceso. Esto servirá para crear una cultura de ciberseguridad que se adapte a la manera de trabajar de hoy día, dando un enfoque principal hacia el patrón CAMS. Se pretende instalar una estrategia de gobierno de ciberseguridad que permita:

- Administrar los recursos de seguridad de manera que la infraestructura generada sea eficaz y eficiente, así como con un coste contenido.
- Instaurar un proceso de mediación del desempeño que permita monitorizar constantemente los procesos de la infraestructura de seguridad para garantizar que se alcancen los objetivos prefijados.

La guía se enfoca principalmente en la transformación de la cultura de ciberseguridad de las empresas. De manera que ésta comprenda todos aquellos comportamientos necesarios para un correcto uso de la tecnología en ámbito de la seguridad de la información.
Como fase previa a la redacción de la guía, se ha realizado una investigación que permitió determinar qué acciones hay que tomar y cómo plantearlas. La investigación ha sido realizada a través de entrevistas al personal de la empresa, las cuales fueron dirigidas, al menos, a un empleado por área. Los resultados de las entrevistas han sido categorizados, y se han formulado métricas adecuadas para generar una evaluación general de la cultura de ciberseguridad de la empresa. Esta evaluación ha sido utilizada cómo bitácora para plantear las acciones futuras. Después de un atento análisis de los resultados de las entrevistas, también por medio de las métricas formuladas, se han planteado e implementado los controles de seguridad necesarios. A través de la monitorización de los controles implementados se han podido analizar y evaluar para instaurar un proceso de mejora continua. Toda la información obtenida por el caso de estudio ha sido finalmente recopilada para redactar la guía.

Keywords: “Cybersecurity Framework”, “Cybersecurity”, “Pyme”, “Guía de controles de seguridad”, “NIST”, “Identify”, “Protect”, “Detect”, “Respond”, “Recover”, “Cloud”, “Analytics”, “Mobile and Social Applications”, “Análisis de riesgos”, “Mejora Continua”, “Gobierno de la seguridad”.

Tabla de contenidos

1. Introducción

1.1 Objetivos del trabajo

El trabajo tiene como objetivo principal la redacción de una guía de ciberseguridad para pequeñas y medianas empresas.

La guía, construida en base al nuevo Cybersecurity Framework de NIST [1]:

Identify

Protect

Detect

Respond

Recover

Fig.1: Logo NIST Cybersecurity Framework

En particular la guía se articula en torno a estos 4 objetivos:

a. Organización estructural ##
b. Cultura de trabajo ##
c. Concienciación de seguridad ##
d. Gobierno de ciberseguridad ##

a) Organización estructural:

- Alineación estratégica que busca un equilibrio entre las medidas de seguridad y las necesidades del negocio.

- Administración de los riesgos que busca mitigarlos y reducir el posible impacto.

b) Cultura de trabajo:

- Creación de una cultura de ciberseguridad que se adapte a la manera de trabajar de hoy día. Dar un enfoque principal hacia el patrón CAMS (Cloud, Analytics, Mobile and Social).

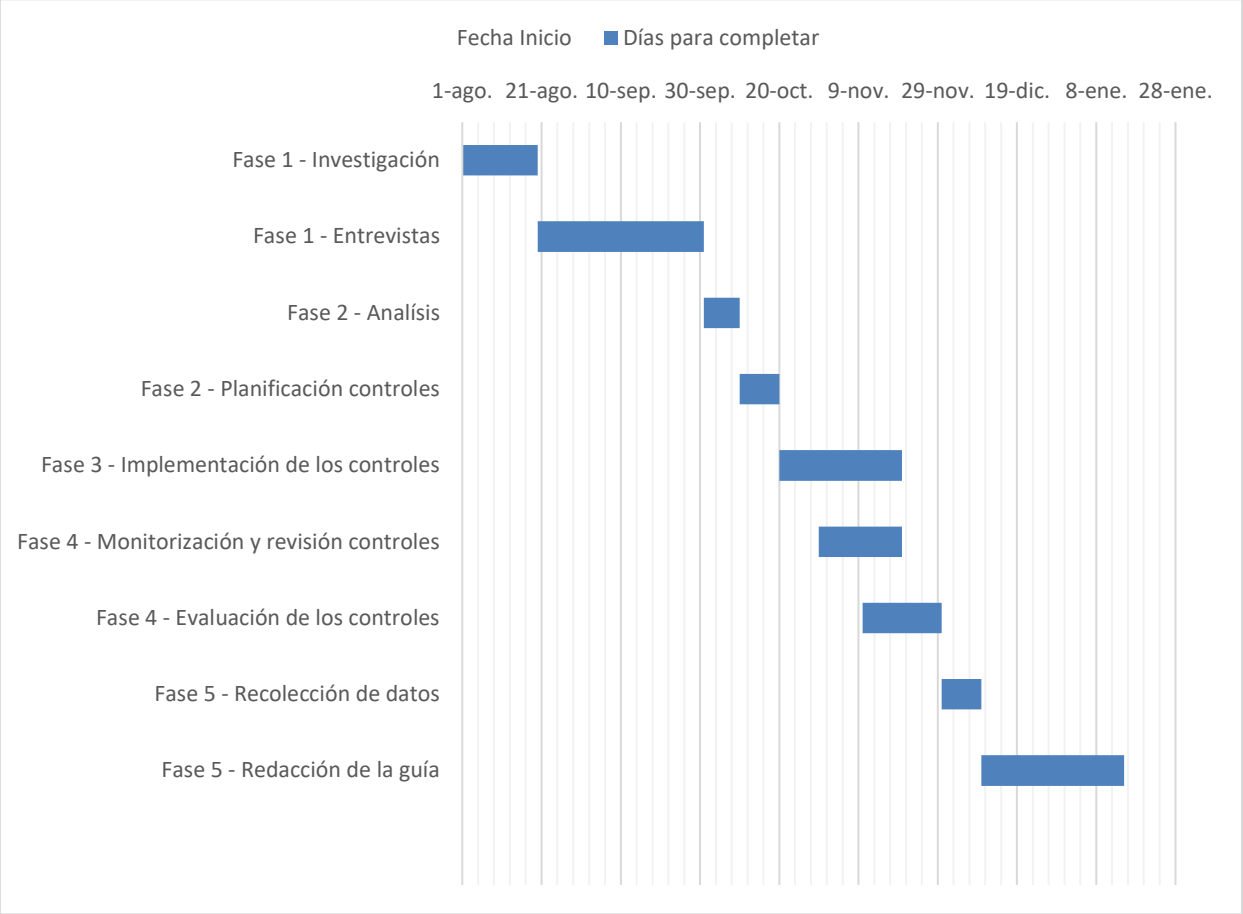
c) Concienciación de seguridad:

- Tratar de concienciar dinámicamente las áreas de la empresa creando programas distintos para cada una de ellas. Esto resultaría en generar mayor interés e implicación del empleado en el programa de concienciación, aumentando eficacia y eficiencia del proceso de concienciación.

d) Gobierno de ciberseguridad:

- Administración de los recursos de seguridad de manera que la infraestructura generada sea eficaz y eficiente.
- Mediación del desempeño: monitorizar los procesos de la infraestructura de seguridad para garantizar que se alcancen los objetivos.
- Integración: garantizar que los procesos de gobierno de seguridad operen correctamente, según la estrategia de gobierno.

1.2 Diagrama de Gantt



1.3 Metodología propuesta

La metodología propuesta se basa en 4 fases principales:

- Investigación
- Medición
- Planificación
- Implementación

La fase de investigación se centra en la recolección de información sobre el estado actual de la organización.
Esta fase se basa en realizar entrevistas al personal de la agencia, en recolectar las respuestas y finalmente categorizarlas según macro-áreas para facilitar sus análisis. Las entrevistas se enfocan en obtener información sobre la cultura de ciberseguridad que existe en la agencia.

La fase de medición se centra en el análisis de la información recolectada, mediante métricas de cultura de ciberseguridad y estándares o normas vigentes en la organización. Esta fase sirve para tomar una foto del estado actual de la agencia, proporcionándonos los principales hallazgos y problemas que iremos a considerar en la fase de planificación.

A través del análisis realizado en la fase de medición, la fase de planificación se centra en planificar aquellas iniciativas que podrían mejorar el estado actual de la organización. Por cada problema o hallazgo detectado en la fase de análisis, se propone una iniciativa que mira también en lograr uno (o más) de los 4 objetivos principales de la guía. Las iniciativas propuestas se categorizan según los pasos del Framework NIST. De esta forma podemos averiguar rápidamente si estamos dejando al descubierto un punto del Framework o nos estamos focalizando en uno en particular sin prestar atención a los demás.

Finalmente, la fase de implementación consiste en adoptar las iniciativas propuestas, dentro de la organización. Las iniciativas implementadas necesitan una monitorización, que permita el desarrollo de un proceso de mejora continua dentro de la agencia. Este proceso es la base de un logro cultural muy importante, que es la cultura de la autoevaluación.

Para poder supervisar la ejecución de las 4 fases y llevar a cabo las iniciativas propuestas, se constituirá un grupo de seguridad. Este último es un órgano fundamental necesario para la gestión de los procesos de seguridad de la información en una organización. La teoría acerca de este tipo de estructura organizativa está basada sobre el modelo BSIMM (Build Security in Maturity Model). Este modelo es el resultado de un estudio plurianual, que se presenta como un estándar de facto para las iniciativas de seguridad de la información en el mundo. El último modelo publicado, el BSIMM9 [2], se construyó a partir de las observaciones recolectadas en 120 firmas y organizaciones.

Según las observaciones que los investigadores han realizado durante años en el proyecto BSIMM, el primer paso de cada iniciativa de seguridad de la información es crear un grupo de seguridad. Entre los dos modelos de grupos de seguridad que el BISMM propone, Software Security Group y Satellite, se ha decidido adoptar el modelo Satellite [3]. Este grupo de seguridad

está compuesto por desarrolladores particularmente interesados en la seguridad del software y por todos aquellos roles que tienen una afinidad especial con la seguridad de la información. Debido a que, 27 de 30 firmas que han obtenido la puntuación más alta en el modelo BSIMM, incorporan esta tipología de grupo de seguridad en su organigrama, un grupo Satellite es un buen índice de madurez para las iniciativas de seguridad de la información.

Supervisar las 4 fases del proyecto requiere sólidos conocimientos y experiencia en el sector de la seguridad de la información para poder garantizar la fiabilidad del estudio y la eficacia de las iniciativas propuestas. Sea por los resultados del estudio BSIMM, sea por poder lograr los 4 objetivos principales del proyecto, la importancia del grupo de seguridad es crítica. La necesidad de poseer el grupo de seguridad de tipo Satellite será descrita en la fase de implementación.

2. Estado del Arte

2.1 Framework NIST

El Cybersecurity Framework de NIST representa un marco normativo de relevancia internacional por lo que concierne la seguridad de la información.

Propone las mejores prácticas de desarrollo de una estrategia de seguridad, proporcionando los controles necesarios a:

- Garantizar la protección de los activos de la organización.
- La gestión de los riesgos que puede estar expuesta la organización
- La correcta implementación de planes de contingencia
- La correcta implementación de planes de continuidad de negocio.

Los controles proporcionados están pensados para organizaciones gobernativas que manejan información sensible y extremamente confidencial. Por eso, basarnos en estos controles para construir una estrategia de seguridad de la información nos garantiza una solución a la vanguardia y con fundamentos sólidos.

2.1.1 NIST

National Institute of Standards and Technology es una agencia del gobierno de Estados Unidos de América. Es parte del Departamento del Comercio y promueve la economía americana a través la colaboración con la industria para desarrollar estándares y metodologías que favorezcan la producción y el comercio. Esta agencia produce estándares de alto nivel en muchos campos de la tecnología. Sus áreas de trabajo e investigación se parecen a los *working groups* de las ISO.

El área que más nos interesa acerca de nuestro proyecto es la de estándares en seguridad de la información. El grupo de estándares que el NIST ha producido sobre este tema es el grupo 800. A través de las más modernas investigaciones en campos de ciencias de la computación, matemática, estadística e ingeniería de sistemas, el programa de ciberseguridad del NIST proporciona soluciones y metodologías que garantizan la interoperabilidad y usabilidad de las mejores prácticas e iniciativas de seguridad de la información en el mundo. Entre las metodologías desarrolladas por el NIST, está el Cybersecurity Framework en el que se basa este proyecto.

2.1.2 El nuevo Cybersecurity Framework

El Framework ha sido publicado en el abril 2018. Contiene nuevos conceptos sobre la creación y la mejora de un programa de ciberseguridad y una nueva sección que explica cómo aplicar el framework a un *self-assessment* del riesgo de ciberseguridad.

2.1.2.1 El riesgo de la ciberseguridad

El riesgo de la ciberseguridad se refiere comúnmente al riesgo financiero, de quiebra o reputacional de una organización a causa de un fallo en el funcionamiento de sus sistemas informáticos. Esto se puede materializar en varias formas:

- Acceso deliberado y no autorizado a los sistemas informáticos de la organización
- Fallos de seguridad no intencionados o accidentales
- Riesgo operacional debido a sistemas informáticos mal configurados

El riesgo de la ciberseguridad no oportunamente gestionado puede conllevar a serias consecuencias que van desde la destrucción de la información importante para la organización hasta llevar esta última a la quiebra.

El riesgo de la ciberseguridad daña la parte principal de una compañía, de igual manera que el riesgo reputacional y financiero. Puede hacer elevar los costes y disminuir los ingresos, dañando la capacidad de innovación y de obtener o retener los clientes.

NIST crea su nuevo Framework precisamente en base la gestión del riesgo de la ciberseguridad. Ralph Langner y Perry Pederson [4] afirman que el problema actual sobre la gestión del riesgo de la ciberseguridad está en el hecho que los managers están incentivados a bajar sus costes. De hecho, mientras el coste de las medidas y de los controles de seguridad está bien definido, no se suele definir el precio de las posibles pérdidas debidas por un fallo de seguridad.

2.1.2.2 Focus del NIST CSF

El Framework NIST pone el foco en el aspecto financiero como timón para guiar las actividades de seguridad de la información, considerando el riesgo de la ciberseguridad parte integrante del sistema de gestión de riesgos en una organización.

El Framework proporciona directrices sobre cómo gestionar la ciberseguridad, a través de estándares y buenas prácticas que actualmente funcionan mejor. Además, refiriéndose a estándares de ciberseguridad reconocidos globalmente, el Framework puede servir como modelo para la cooperación internacional a la hora de fortalecer la seguridad de la información.

Manteniéndose tecnológicamente neutro, sigue siendo siempre válido fomentando la innovación técnica.

El núcleo del framework se desarrolla en las 5 funciones continuas y concurrentes:

- Identify
- Protect
- Detect
- Respond
- Recover

Todas juntas las cinco funciones proporcionan una visión estratégica a alto nivel del ciclo de vida de la gestión del riesgo de la ciberseguridad en la organización.

2.2 Estrategias de Ciberseguridad para PYME

En la realización del proyecto se toman en cuenta dos modelos de ciberseguridad para pyme que tienen relevancia en el estudio de investigación y en la redacción de la guía.

El Instituto Nacional de Ciberseguridad de España (INCIBE) [5] propone un modelo que está basado en una guía publicada por el Communications-Electronics Security Group **(**CESG) británico. Esta guía está compuesta por 10 puntos clave:

1. Comprender y gestionar los riesgos:
   Es necesario designar un responsable de la gestión del riesgo de la ciberseguridad dentro de la agencia. El rol del responsable será encargado de:
   a. Redactar de un listado de los pasos necesarios para la gestión del riesgo de la ciberseguridad.
   b. Definir el nivel de riesgo que se está dispuestos a aceptar.
2. Actualizar el software:
   Es necesario poner particular atención en que todos los activos informatizados de la organización estén actualizados a su última versión estable.
3. Proteger la red:
   Es necesario instalar y configurar un firewall en la red de la organización.
4. Instalar defensas antimalware:
   Es necesario que en todos los dispositivos de la organización esté presente un antimalware o un paquete de seguridad del software que incluya esta funcionalidad.
5. Gestionar el acceso a los sistemas (privilegios de usuarios):
   Es necesario aplicar el principio del mínimo privilegio en la asignación de los permisos de acceso a los sistemas de la organización.
6. Controlar los dispositivos removibles:
   Vigilar el uso de dispositivos externos removibles y realizar escaneos cada vez que se utilicen.
7. Monitorizar las redes y servicios:
   Instalar un paquete de monitorización de la red para detectar comportamientos anómalos o malévolos de los usuarios.
8. Enseñar las buenas prácticas (formación de usuarios)
   Es necesario garantizar que todos los empleados conozcan la política de seguridad y sobre todo que se presente a los nuevos.
9. Controlar los dispositivos móviles de propiedad de la empresa
   Es necesarios que los dispositivos móviles de la empresa que utilizan los trabajadores estén dotados de medidas de seguridad como cifrado de memoria y un mejor patrón de acceso.
10. Gestionar los incidentes y la continuidad de negocio
    Diseñar, implantar y monitorizar un plan de continuidad de negocio

2.3 Metodologías de Transformación Cultural

Para la realización de este proyecto se ha tomado en cuenta la metodología de trasformación cultural presentada por la agencia de la redes y seguridad informática de la Unión Europea (ENISA).

La agencia muestra como a pesar de que las políticas de seguridad son actualmente un estándar para todas las compañías modernas, en la mayoría de los casos de pérdidas o filtración de datos los causantes son las personas. Esto hace pensar que sea posible que estas personas no vean las políticas como un conjunto de reglas, sino como directrices que no están obligados a observar.

La solución propuesta es de hecho construir e implantar una cultura de ciberseguridad que pueda lograr un cambio de mentalidad y favorezca la concienciación de la ciberseguridad y la percepción de los riesgos, en lugar de imponer un "comportamiento seguro". La cultura de ciberseguridad de una organización se refiere a los conocimientos, creencias, percepciones, actitudes, suposiciones, normas y valores de las personas relacionadas con la ciberseguridad y cómo se manifiestan en el comportamiento de las personas que manejan tecnología informática. La cultura de ciberseguridad trata de hacer que las consideraciones de seguridad de la información sean parte integrante del trabajo, los hábitos y la conducta de un empleado, integrándolos en sus acciones diarias. Adoptar el enfoque adecuado para la seguridad de la información permite a la cultura desarrollarse naturalmente a partir de los comportamientos y actitudes de los empleados hacia los activos de información en el trabajo, y como parte de la cultura organizativa más amplia de la empresa.

Sin embargo, los entornos empresariales cambian constantemente, por lo tanto, las organizaciones deben mantener y adaptar activamente su cultura de ciberseguridad en respuesta a las nuevas tecnologías y amenazas, así como sus objetivos, procesos y estructuras organizativas. Una cultura de ciberseguridad exitosa da forma al pensamiento de seguridad de todo el personal (incluido el equipo de seguridad), mejorando la resiliencia contra todas las ciber amenazas, especialmente cuando se inician a través de la ingeniería social, evitando imponer medidas de seguridad onerosas que impidan que el personal desempeñe eficazmente sus principales funciones.

2.3.1 Métricas de la cultura de la ciberseguridad

En particular, ENISA en la publicación "Cyber Security Culture in organisations" (2017) [6] hace referencia clara a un estudio realizado por CLTRe [7] para soportar su metodología de creación de cultura de ciberseguridad. El estudio denominado Security Culture Report de CLTRe muestra los resultados de las mediciones de la cultura de la ciberseguridad en varias agencias europeas.

La metodología de CLTRe se basa en la investigación científica del comportamiento organizativo (Ajzen, 2011) [8] que demuestra como el comportamiento humano no depende solo de su conocimiento, sino en particular manera de la cultura en la organización, su normas y costumbres.

CLTRe afirma que, para medir el aspecto cultural de ciberseguridad, se ha abusado de métricas de vanidad como por ejemplo el número de participantes a un curso de concienciación de ciberseguridad o su tasa de finalización. Las métricas parecen buenas en primer análisis, pero no miden el efecto de estas actividades. En cambio, fomenta el uso de métricas que puedan medir el efecto de una actividad específica o un programa. El CLTRe identifica 7 métricas principales sobre las cuales basa su medición de la cultura de la ciberseguridad:

- **Comportamientos**: actividades reales o previstas y acciones de alto riesgo de los empleados que impacte directa o indirectamente con la cultura de ciberseguridad.
- **Actitudes**: sentimientos e opiniones de los empleados de cara a las actividades propuestas sobre la seguridad en la organización.
- **Conocimiento**: conocimientos y creencias de los empleados relacionados con la seguridad en la organización.
- **Cumplimiento**: alineamiento e incongruencias con la política de seguridad, saber que existe y poder nombrar algunos de sus pilares/puntos.
- **Comunicación**: maneras en que los empleados se comunican entre ellos, sentido de pertenencia, responsabilidad y capacidad de reportar incidentes.
- **Normas**: percepción de cuál sería un adecuado/normal comportamiento de cara a un reglamento o conducta de seguridad en la organización y que prácticas en cambio serían "malas".
- **Responsabilidades**: conciencia de que cada empleado es un factor crítico en soportar o amenazar a la seguridad de la organización.

2.4 Estándares en Controles de Seguridad

Para la realización del proyecto se han tenido en cuenta los controles, sistemas de gestión y frameworks propuestos por tres entidades que se ocupan de: estudiar, establecer y mejorar los estándares en la seguridad de la información en el mundo.

2.4.1 NIST 800-53 [9]

Los controles de seguridad propuestos por esta publicación del NIST son entendidos como contramedidas prescritas para los sistemas informáticos u organizaciones que fueron diseñados para:

- Proteger la confidencialidad, integridad y disponibilidad de la información que se procesa, almacena y trasmite;
- Satisfacer un conjunto de requerimientos de seguridad de la información, derivados de necesidades del negocio, leyes, ordenes ejecutivos, directivos, regulatorios, políticas y estándares.

El objetivo de esta publicación es proporcionar las directrices para seleccionar y establecer controles de seguridad para que las organizaciones y los sistemas informáticos cumplan con los requisitos mínimos de seguridad para la información. Además de los controles, esta publicación proporciona:

1. Un conjunto de controles para la gestión de programas de seguridad de la información (PM) que normalmente se implementan a nivel organizacional y no se dirigen a sistemas de información individuales;
2. Un conjunto de controles de privacidad basados en estándares internacionales y mejores prácticas que ayudan a las organizaciones a hacer cumplir los requisitos de privacidad derivados de la legislación federal, directivas, políticas, reglamentos y normas;
3. Establece un vínculo y una relación entre los controles de privacidad y seguridad a efectos de hacer cumplir los respectivos requisitos de privacidad y seguridad, cuya teoría e implementación pueden superponerse dentro de los sistemas de información, programas y organizaciones.

2.4.2 ISO 27001 [10]

Es un estándar internacional cuyo objetivo es proporcionar un modelo para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI). La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación de la SGSI de una organización está influenciado por sus necesidades y objetivos, los requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Cualquier actividad que utilice recursos y se administra para permitir la transformación de entradas en salidas puede considerarse un proceso. El estándar adopta un enfoque de proceso para la gestión de la seguridad de la información que alienta a sus usuarios a enfatizar la importancia de:

a) comprender los requisitos de seguridad de la información de una organización y la necesidad de establecer políticas y objetivos de seguridad de la información;

b) implementar y operar controles para gestionar los riesgos de seguridad de la información de una organización en el contexto de los riesgos empresariales generales de la organización;

c) supervisar y revisar el desempeño y la efectividad del SGSI;

d) mejora continua basada en la medición objetiva. En particular adopta el modelo "Plan-Do-Check-Act" (PDCA), que se aplica para estructurar todos los procesos de SGSI.

2.4.3 BSIMM 9

El propósito de la BSIMM es cuantificar las actividades llevadas a cabo por iniciativas reales de seguridad del software. Debido a que estas iniciativas utilizan diferentes metodologías y terminología diferente, el BSIMM requiere un framework que les permite describir todas las iniciativas de manera uniforme. Este framework de seguridad de software (SSF) y las descripciones de las actividades proporcionan un vocabulario común para explicar los elementos relevantes de una iniciativa de seguridad del software (SSI), por lo tanto, nos permite comparar iniciativas que utilizan diferentes términos, operan a diferentes escalas, existen en diferentes mercados verticales, o crean diferentes productos.

El estudio se clasifica como un modelo de madurez porque mejorar la seguridad del software casi siempre significa cambiar la forma en que funciona una organización, y esto no es inmediato. Precisa que no todas las organizaciones alcanzan los mismos objetivos de seguridad, pero afirma que todas las organizaciones pueden beneficiarse del uso de la misma varilla de medición.

BSIMM9 es la novena versión principal del modelo. Incluye descripciones actualizadas de la actividad, datos de 120 organizaciones.

La metodología usada por BSIMM en construir su modelo es la siguiente:

- Se generó el framework de seguridad del software (SSF) [11], identificando 12 practicas principales y organizándolas en cuatro áreas de interés:

    - Gobernanza:
        - Estrategia y métricas
        - Cumplimiento y políticas
        - Entrenamiento
    - Inteligencia:
        - Modelos de ataque
        - Características y diseño de la seguridad
        - Estándares y requerimientos
    - Ciclo de vida del Desarrollo del Software Seguro:
        - Análisis arquitectural
        - *Code Review*
        - Pruebas de seguridad
    - Despliegue:
        - *Penetration Testing*
        - Entornos de software
        - Gestión de configuraciones y vulnerabilidades

- Se realizaron una serie de entrevistas en persona con nueve ejecutivos a cargo de SSIs. De estas entrevistas, se identificaron un conjunto de actividades comunes, que organiza de acuerdo con el SSF.
- Luego se creó un cuadro para cada una de las nueve iniciativas que muestran las actividades que llevan a cabo.
- Para validar el estudio, se ha finalmente pedido a cada empresa participante que revise el framework, las prácticas y el cuadro creado para sus iniciativas.

2.5 Estándares en Gobierno de Seguridad

2.5.1 ISACA COBIT 5 [12]

ISACA con COBIT5, hace hincapié en la importancia de separar el gobierno y la gestión de la seguridad de la información. De particular manera en lo que respecta la creación de un

Framework único para el gobierno de la seguridad de la información afirmando que es oportuno considerar:

1. La ciberseguridad como definida en la ISO 27032 [13].
2. Los Top 20 controles críticos que ilustra SANS [14].
3. Los Framework existentes en la gestión de riesgos y de buenas prácticas que afectan la seguridad de la información.
4. Los modelos de planes de continuidad de negocio y de nivel de gobierno definidos en la ISO 27301 [15].
5. La estructura organizativa o corporativa de la propia agencia.

En concreto propone un conjunto de funciones y conceptos basados en tres fases principales:

1. Evaluación
2. Dirección
3. Monitorización

El proceso de evaluación se debe aplicar al marco normativo, regulatorio y contractual vigente, así como los requerimientos del negocio, para poder generar un modelo óptimo de toma de decisión para la seguridad de la información.

El objetivo principal del proceso de dirección es implementar y gestionar todas aquellas iniciativas que permiten alinear la estrategia de seguridad con las necesidades del negocio, fomentar una cultura y un entorno positivo en la seguridad de la información.

El proceso de monitorización establece la formulación de las métricas necesarias para poder analizar con facilidad las posibles complicaciones que pueden surgir en el programa de seguridad de la información dado el continuo cambio del panorama de la ciberseguridad.

2.5.2 NIST 800-100[16]

Sobre el lado de la estrategia de gobierno de seguridad de la información establece dos modelos principales:

- Centralizado
- Descentralizado

Añade, además, que una implementación del gobierno de la seguridad completamente centralizada o descentralizada es bastante difícil de encontrar. De hecho, las agencias tienden a adoptar una estrategia híbrida que les permita adaptar el modelo a su dimensión, misión y/o cualesquiera estructuras de gobierno de seguridad actual.

Para definir esos modelos, proporciona las especificaciones para 3 figuras fundamentales para la organización estructural del gobierno de la seguridad de la información:

Agency Head: es el elemento estructural en el escalón más alto, es responsable de todos los procesos que garantizan la seguridad de la información en la agencia; además tiene la responsabilidad de designar un CIO (Chief Information Officer), y garantizar que el anualmente

presente un informe sobre la eficacia del programa de seguridad, incluyendo su progreso en las eventuales acciones correctivas realizadas.

CIO: Designado directamente por el Agency Head, esta al cargo del diseño, de su siguiente implementación y del mantenimiento del programa de seguridad de la información. Tiene además la tarea de designar el Senior Agency Information Security Officer (SAISO). En otros contextos organizativos esta figura se llama también Chief Security Officer(CSO) o Computer Informacion Security Officer (CISO).

SAISO, CSO, CISO: Designado por el CIO está a cargo de todos los servicios relativos a la seguridad de la información en la agencia. Es responsable de: la monitorización de todos los procesos del programa de seguridad de la información; implementar nuevos procesos y actividades; mejorar los que ya existen; asegurar que el personal este adecuadamente calificado para realizar sus funciones; proporcionar soporte al CIO en la redacción del informe anual sobre la eficacia del programa de seguridad de la información.

De acuerdo con la dimensión de la agencia, existirán otros roles segundarios al SAISO el cual se encargará de designar y gestionar. En el caso de una PYME esto podría no ser necesario, ya que el programa de seguridad de la información, en estos casos, es más fácil de gestionar.

3. Fase de Investigación

En la fase de investigación se ha procedido a realizar entrevistas para obtener información sobre el estado actual de la ciberseguridad en la organización.

La parte más importante de la fase de investigación es la realización de las entrevistas. Por tanto, la creación de la base de datos de las preguntas es un proceso de igual criticidad. El objetivo de esta primera fase del proyecto es capturar una instantánea del estado actual de la agencia relativo a la seguridad de la información. Se quiere incluir en esta fase el número mayor de entrevistados posibles de forma que esta instantánea tenga una buena fiabilidad.

Para que esto sea posible se ha puesto como requisito fundamental que las entrevistas involucren por lo menos un empleado por área o proceso de la agencia. Como requisito adicional, allí donde en un proceso sea presente una organización multinivel, se ha considerado necesario involucrar la figura que ocupa la posición de más alto nivel.

Vamos a definir y describir los varios procesos de esta fase.

3.1 Creación de la base de datos de preguntas

El objetivo de este proceso es crear una base de datos de preguntas que pueda ayudar en la mejor manera a representar un estado actual de las nociones, comportamientos y aspectos culturales relativos a la seguridad de la información en la agencia. Para el caso de estudio conducido, el grupo Satellite participa en la primera fase de ideación de las preguntas.

Nos interesa particularmente saber que nociones poseen los empleados acerca de:

- La importancia del riesgo de la ciberseguridad en las agencias modernas;
- Las técnicas principalmente utilizadas en el cibercrimen actualmente;
- La importancia de proteger los datos más sensibles;
- La importancia de poder clasificar los datos como sensibles;
- La importancia de conocer el marco normativo vigente dentro de la agencia;
- El valor de los activos que se manejan y producen.

El listado presenta las principales áreas de interés para poder investigar sobre los aspectos culturales de la seguridad de la información.

Se ha aprovechado de la multidisciplinariedad de los componentes del grupo Satellite para obtener una rica variedad de preguntas de manera rápida. Teniendo en cuenta el listado de las áreas de interés principal para el proyecto, hemos decidido organizar un *brainstorming*. Cada componente del grupo Satellite, considerando su área de especialización, ha propuesto interrogantes para cada punto del listado. El grupo ha sucesivamente procesado las preguntas para adaptar el lenguaje técnico a uno más coloquial y accesible a todos los entrevistados. Si dos o más miembros del grupo propusieron la misma pregunta se trató de elegir la más completa o de completarla juntando los elementos de las dos.

3.1.1 Categorización de las preguntas

Puesto que las preguntas han sido generadas a través de un proceso de *brainstorming* fue necesaria su siguiente categorización para que fueran aplicables de manera sencilla en las entrevistas.

Se han generado las siguientes categorías:

1. Cyber Higene:
   Esta categoría recoge todas aquellas preguntas relativas al uso diario de los aparatos informáticos personales o de la agencia. Especialmente su uso, protección y control. De esta categoría forman parte interrogantes sobre: uso de claves de accesos más o menos complejas, políticas de BYOD (Bring Your Own Device) [19], uso de software que analiza la integridad de los dispositivos (antivirus, antimalware, escaneos de vulnerabilidades).
2. Responsabilidades:
   Esta categoría recoge todas aquellas preguntas relativas al rol de los entrevistados dentro de la agencia, y su percepción a respecto. De esta categoría forman parte interrogantes sobre: comunicación, intercambio y responsabilidades de la información que el entrevistado maneja.
3. Valor de los activos:
   Esta categoría recoge los interrogantes sobre el valor percibido de los activos de la agencia. De esta categoría forman parte interrogantes sobre: valor intrínseco de la información que el entrevistado maneja directamente y de los activos más importantes dentro de toda la agencia.
4. Cultura de la ciberseguridad:
   Esta categoría recoge todos aquellos interrogantes relativos a los conceptos generales de seguridad de la información. De esta categoría forman parte preguntas sobre: definición e identificación de las amenazas principales, habilidad de clasificación de los riesgos más comunes y sobre el concepto de seguridad de la información en sí.
5. Actitudes:
   Esta categoría recoge las preguntas relativas a la predisposición del entrevistado en participar en pruebas, iniciativas o cursos relativos a la seguridad de la información en la agencia.

3.2 Realización de las entrevistas

Se ha decidido realizar las entrevistas por área de manera que se pudiese obtener una visión general de la condición de la concienciación en materia de seguridad para cada proceso organizacional y ejecutivo. Las entrevistas se realizaron a colaboradores de las áreas de tecnología, administración y finanzas, directorio y gestión de proyectos.

3.2.2 Estructura de la entrevista

Cada entrevista tuvo una duración aproximada de 40 minutos. Se han sido presentes dos entrevistadores, alternándolos entre los componentes del grupo Satellite de seguridad. Antes de empezar la entrevista se procedió a explicar a grandes rasgos el objetivo del proyecto y de las entrevistas en particular. Se grabaron las entrevistas de manera que fue posible volver a escucharlas en un segundo momento y registrar las respuestas con una mayor exactitud.

Durante la entrevista se realizaron las preguntas por categoría, tratando de no seguir el mismo esquema todas las veces. Lo último, para evitar que las respuestas brindadas puedan ser sugestionadas por el orden de las preguntas. Además, durante la entrevista no se sugirieron las respuestas a los entrevistados con el objetivo de garantizar las respuestas genuinas.

No siempre se realizaron todas las preguntas presentadas en la base de datos, se eligieron algunas por cada categoría antes de iniciar la entrevista. La entrevista no es un examen, el entrevistado no se debe sentir evaluado o estudiado. El objetivo es conocer, en la manera más genuina posible, como la seguridad de la información afecta su día día en el entorno laboral y personal. De hecho, siendo un tema también cultural, saber cómo el entrevistado se comporta en el entorno personal nos puede ayudar mucho en entender sus hábitos en materia de seguridad.
Generalmente quien posee una buena actitud hacia la seguridad informática y adopta un comportamiento seguro en un entorno personal, también aplica estos hábitos en el entorno laboral.

3.3.3 Redacción informe de la entrevista

Una vez terminada la entrevista, se procederá a complementar los apuntes con las grabaciones de voz. Es así que se tendrá un resumen exhaustivo de las respuestas del entrevistado. Es muy importante elaborar este resumen poco tiempo después de terminada la entrevista, ya que se puede enriquecer el documento con los propios recuerdos del entrevistador y sus impresiones durante el proceso. Cuando se termina el registro, cada miembro del equipo de seguridad tiene una forma de lectura diferente de acuerdo con su propia experiencia, ya sea académica o laboral, para interpretar las respuestas.

3.3 Categorización de las respuestas

Las entrevistas han revelado los hábitos, el conocimiento y la mentalidad de los empleados acerca de la seguridad de la información.

Principalmente para la información que cada empleado maneja hemos analizado el Valor, el Impacto y la Confidencialidad. Con el objetivo de medir si el valor atribuido corresponde o tiene correlación con el impacto y la confidencialidad que tiene cada uno de los entrevistados.

Además, hemos analizado el nivel de concienciación y de conocimiento de cada empleado sobre los conceptos generales de seguridad informática.
Asimismo, con el propósito de obtener datos homogéneos, las respuestas de los entrevistados han sido divididas en categorías para lograr un análisis más preciso y facilitar la lectura.

Hemos identificado seis categorías principales que nos ayudan en el análisis:

1. Valor de la información que posee/maneja:
   Recopila toda la información sobre el valor que el entrevistado atribuye a la información que maneja. Que información considera más valiosa y por qué.

2. Valor de la información personal:
   Recopila todas las respuestas acerca del valor que el entrevistado atribuye a su información personal.

3. Confidencialidad de la información que posee/maneja:
   Recopila todas las respuestas acerca de cómo el entrevistado cuida la información que maneja, el cómo y por qué la cuida y la protege.

4. Impacto de la pérdida de la información que posee/maneja:
   Recopila las respuestas acerca de cuál sería, según el entrevistado, el impacto de un eventual robo, pérdida o disrupción de la información que maneja o posee.

5. Conceptos de seguridad de la información generales:
   Recopila todas aquellas respuestas a interrogantes sobre ataques informáticos, incidentes de seguridad, navegación segura, contraseñas seguras,

6. Nivel de concienciación:
   Recopila todas aquellas informaciones sobre las buenas prácticas en la seguridad de la información.

Mediante estas categorías iremos construyendo nuestra estrategia de análisis, armando métricas y indicadores para medir las respuestas de los entrevistados. Durante una entrevista tratamos de hacer por lo menos una pregunta por cada categoría identificada, de forma que los resultados de las distintas entrevistas sean los más homogéneos posible. Desafortunadamente

esto no siempre ha sido posible porque el entrevistado puede decidir si contestar o menos a una pregunta. Aunque cada respuesta es muy importante para la investigación, no queremos que los entrevistados se sientan de alguna forma examinados por el grupo de seguridad. De hecho, no queremos el nivel de estrés de los entrevistados aumente durante las entrevistas, ya que esto podría conllevar a que el trate de defenderse no respondiendo verídicamente. Para esta razón, hay que poner bien claro sin desde el inicio de la entrevista que las respuestas no estarán compartidas con los jefes directos del entrevistado si no de forma anónima, generalizada o con finalidad puramente estadística.

4. Fase de análisis

En la fase de análisis hemos estudiado las respuestas recogidas en las siete categorías identificadas.

4.1 Definición de las métricas

Para realizar este análisis, se ha decidido adoptar las 7 métricas de la cultura de la ciberseguridad de CLTRe para alinearlas a nuestros 4 principales objetivos: Organización estructural, Cultura de trabajo, Concienciación de seguridad, Gobierno de la ciberseguridad.

La cultura de la ciberseguridad es considerada como la piedra angular de la seguridad en las organizaciones. En pocas palabras, se trata de internalizar los problemas de seguridad en el trabajo de cada empleado. Se trata de adoptar hábitos seguros y poder tomar decisiones orientadas a la seguridad. A pesar de que las más modernas medidas de seguridad tecnológicas permiten un control siempre mayor sobre los sistemas, son los mismos trabajadores que inconscientemente producen fallas en la seguridad y esto es un resultado de una cultura de ciberseguridad inmadura o escasamente desarrollada.

Los indicadores de la cultura de ciberseguridad son tan importantes como la calidad de las soluciones IT para proteger la seguridad de una organización. En particular miden:

1. La predisposición en adoptar y participar en iniciativas de seguridad, representado por el indicador **Actitudes**.

2. Cómo los empleados perciben su rol en la organización, representado por el indicador **Responsabilidades**

3. Conciencia y capacidad de usar canales de informe o reporte de problemas, representado por el indicador **Comunicación**

4. La adhesión y el cumplimiento con las normativas y políticas de la organización está representado por el indicador **Cumplimiento**

5. El conocimiento de los asuntos relativos a la seguridad está representado por el indicador **Conocimientos**

6. Cómo los empleados ven las acciones de los demás o cómo sus acciones están influenciadas por sus pares es representado por el indicador **Normas**

7. Las acciones que los mismos empleados realizan, representado por el indicador **Comportamientos**

4.1.1 Producción de la escala de evaluación

Cada métrica está expresada en un rango del 1 al 5. Siendo 1 el grado más bajo de cumplimiento, casi nulo; y 5 el grado más alto y óptimo.

Definir los niveles nos permite cuantificar el cumplimiento de nuestros principales 4 objetivos:

- Las métricas de Comportamientos, Actitudes y Normas nos permiten medir la Cultura de Trabajo
- Las métricas de Responsabilidades y Cumplimiento nos permiten medir el Gobierno de la Ciberseguridad
- Las métricas de Conocimientos y Comportamientos nos permiten medir la Concienciación de seguridad
- Las métricas de Comunicación y Responsabilidades nos permiten medir la Organización Estructural

Cada empleado obtendrá una puntuación basada en su entrevista y las preguntas que contestó. Las métricas son acciones que van siendo más y más adecuadas para lograr nuestros objetivos progresivamente con el nivel correspondiente.

Las métricas formuladas se desarrollan en los siguientes niveles:

Comportamientos	
1	No utiliza ningún sistema de protección; No tiene conocimientos de riesgos básicos (Robo de datos, malwares)
2	No utiliza ningún sistema de protección; Tiene conocimientos de riesgos básicos (Robo de datos, malwares)
3	Utiliza sistemas de protección básicos (Password, Navegación bajo TLS, Antivirus Free); Tiene conocimientos de riesgos básicos (Robo de datos, malwares)
4	Utiliza sistemas de protección básicos (Password, Navegación bajo TLS, Antivirus Free); Tiene conocimientos de riesgos avanzados (Categorías de malware, acceso libre a datos sensibles/privados, spear phishing)
5	Utiliza sistemas de protección avanzados (Password managers, Navegación bajo proxy VPN, Anti malware&spyware, Role Based Access Control (RBAC) para sus datos sensibles/privados); Tiene conocimientos de riesgos avanzados (Categorías de malware, acceso libre a datos sensibles/privados, spear phishing)

Actitudes	
1	Está indiferente con las actividades propuestas sobre la seguridad; No participa activamente en las actividades

2	No está de acuerdo en realizar las actividades propuestas sobre la seguridad en la organización; No participa activamente en las actividades
3	No está de acuerdo en realizar la mayoría de las actividades propuestas sobre la seguridad en la organización; Participa activamente en las actividades
4	Está de acuerdo en realizar la mayoría de las actividades propuestas sobre la seguridad en la organización; Participa activamente en las actividades
5	Está de acuerdo en realizar todas las actividades propuestas sobre la seguridad en la organización; Participa activamente en las actividades

Conocimiento	
1	Cree que la seguridad informática es solo responsabilidad del departamento de tecnología, no conoce los principales vectores de ataque y no sabe cómo protegerse.
2	Cree que la seguridad informática es solo responsabilidad del departamento de tecnología, conoce los principales vectores de ataque, pero no sabe cómo protegerse.
3	Cree que la seguridad informática es solo responsabilidad del departamento de tecnología, sabe cómo protegerse de los principales ataques informáticos, no conoce vectores avanzados/modernos de ataque.
4	Cree que la seguridad informática es responsabilidad de todos, sabe cómo protegerse de los principales ataques informáticos, conoce vectores avanzados/modernos, pero no sabe cómo protegerse.
5	Cree que la seguridad informática es responsabilidad de todos, sabe cómo protegerse de los ataques avanzados y modernos.

Cumplimiento	
1	Desconoce reglas y políticas de seguridad de la información
2	Conoce algunas reglas y políticas de seguridad de la información, pero no siempre las respeta.
3	Conoce algunas reglas y políticas de seguridad de la información y las respeta.
4	Conoce la mayoría de las reglas y políticas de seguridad de la información y las respeta.
5	Conoce la totalidad de las reglas y políticas de seguridad de la información y las respeta.

Comunicación	
1	No sabe identificar un activo sensible, no filtra la información que comunica, no sabe identificar un peligro entonces no puede comunicarlo.
2	No sabe identificar un activo sensible, filtra la información que comunica a través del sentido común, no sabe identificar un peligro entonces no puede comunicarlo.
3	No sabe identificar un activo sensible, filtra la información que comunica a través del sentido común, sabe identificar un peligro entonces puede comunicarlo, aunque no sabe calcular el riesgo.
4	Sabe identificar un activo sensible, filtra la información que comunica en base a su sensibilidad, sabe identificar un peligro entonces puede comunicarlo, aunque no sabe calcular el riesgo.
5	Sabe identificar un activo sensible, filtra la información que comunica en base a su sensibilidad, sabe identificar un peligro y calcular su riesgo entonces puede comunicarlo.

Normas	
1	No sabe cómo distinguir una práctica buena de una mala, no basa sus acciones en ninguna norma específica. Sus conocimientos son básicos o nulos.
2	No sabe cómo distinguir una práctica buena de una mala, basa sus acciones en el sentido común. No tiene experiencia ni conocimientos de buenas prácticas en la seguridad informática
3	Distingue buenas y malas prácticas mediante el sentido común y su experiencia. Tiene conocimientos limitados sobre normas y buenas prácticas en la seguridad de la información.
4	Distingue buenas y malas prácticas evaluando las consecuencias de sus acciones mediante su experiencia y conocimientos limitados.
5	Sabe cómo distinguir buenas y malas prácticas a través de las consecuencias de sus acciones. Tiene experiencia y conocimientos avanzados sobre normas y buenas prácticas en la seguridad de la información.

Responsabilidades	
1	No sabe determinar el nivel de responsabilidad de su rol individual.
2	Sabe determinar el nivel de responsabilidad de su rol individual en situaciones comunes. Tiene conocimientos básicos o nulos sobre políticas y buenas prácticas. No aplica sus conocimientos a su entorno laboral.
3	Sabe determinar el nivel de responsabilidad de su rol individual en situaciones comunes. Tiene conocimientos limitados sobre políticas, buenas prácticas, métricas y procedimientos. No sabe todavía aplicarlos a su entorno laboral.

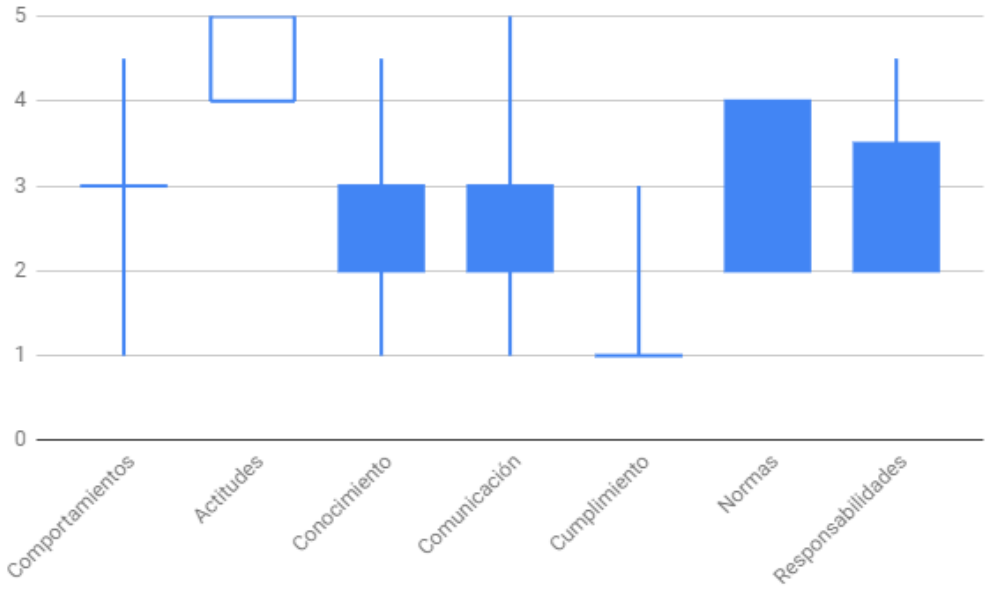
4	Sabe determinar el nivel de responsabilidad de manera apropiada a su rol individual. Tiene conocimientos avanzados sobre políticas, buenas prácticas, métricas y procedimientos, no sabe todavía aplicarlos adecuadamente a su entorno laboral.
5	Sabe determinar el nivel de responsabilidad de manera apropiada a su rol individual. Tiene conocimientos avanzados sobre políticas, buenas prácticas, métricas y procedimientos, y sabe aplicarlos adecuadamente a su entorno laboral.

4.2 Visualización de los resultados

Una vez medidos los indicadores de la cultura de la ciberseguridad continuamos con la fase *plotting.*

En el grafico siguiente podemos ver las puntuaciones obtenidas por los empleados entrevistados agrupadas por indicador de cultura de la ciberseguridad. El grafico nos ayuda para un análisis rápido y superficial que nos servirá como punto de partida para nuestro estudio.

	Mean	StDev	Min	Max
Comportamientos	3	1,3	1	4,5
Actitudes	5	0,3	4	5
Conocimiento	3	1,2	1	4,5
Comunicación	2	1,4	1	5
Cumplimiento	1,5	1,1	1	4
Normas	2,5	1,1	2	4,5
Responsabilidades	2,75	1	2	4,5



De la gráfica podemos deducir que la empresa presenta una fortaleza en el indicador de Actitudes y una debilidad en Cumplimiento. Estos datos de por si no son valiosos, de hecho, necesitamos una escala de evaluación para interpretarlos y una forma de comparar los resultados con un marco de referencia.

Para la interpretación de la puntuación de cada indicador, utilizaremos una escala cualitativa basada en los niveles precedentemente establecidos. Una evaluación cualitativa nos ayuda atribuyendo un sentido fácilmente interpretable a los números. Además, nos permiten expresar en palabras el nivel de cultura de seguridad medio de una empresa y, por lo tanto, su grado de madurez.

Vamos a representar las puntuaciones en una escala de 6 valores cualitativos:

1. Peligro muy alto (0 - 1)
2. Peligro alto (1 - 2,5)
3. Problemático (2,5 - 3)
4. Inseguro (3 - 4)
5. Satisfactorio (4 - 4,5)
6. Ejemplar (4,5 - 5)

Para poder comparar los resultados vemos a usar un gráfico de tipo radar. Este tipo de gráfico es apto para mostrar la puntuación agrupada por categoría, además, tiene también la posibilidad de mostrar varias muestras y compararlas al mismo tiempo. El uso de este gráfico no solo es útil para comparar los datos, lo es sobre todo para visualizar la tendencia de los indicadores. El objetivo es que el gráfico que vamos a dibujar funcione como brújula para las iniciativas de seguridad que propondremos y sucesivamente implementaremos. A través de mediciones continuas podremos medir el efecto que las iniciativas tendrán sobre la cultura de la ciberseguridad en la organización. En particular se buscará mantener el polígono lo más regular posible para garantizar un equilibrio en los indicadores [17].

Los ejes de un gráfico tipo radar son orientados radialmente. Poseen tantos ejes como categorías que queremos medir y tantos círculos como niveles haya para cada categoría. Los niveles se desplazarán concéntricamente partiendo del nivel 1, el más interno, hacia el nivel 5, el más externo.

Para el análisis de los resultados de nuestra investigación vamos a usar este grafico para agrupar los resultados singulares de cada empleado por categorías. Esto nos servirá para:

- Evidenciar diferencias importantes para nuestro estudio entre los empleados.
- Encontrar patrones categorizados por áreas de trabajo.
- Evidenciar deficiencias en las métricas en relación con los resultados obtenidos en otras empresas en el mundo.

4.3 Principales hallazgos

A través del análisis de los gráficos obtenidos hemos extrapolado los principales hallazgos sobre la cultura de ciberseguridad entre los empleados de la agencia:

1. La cultura de la ciberseguridad de los empleados no es homogénea, existe una brecha muy amplia entre roles y funciones. Principalmente entre el área de tecnología y el resto.
2. Los empleados en general consideran que la información que poseen o manejan no es valiosa o no merece una protección formal. Muchos no conocen sus responsabilidades sobre la misma, ya sean morales o legales. La mitad de los entrevistados no tenían idea que existieran acuerdos de confidencialidad con los clientes.
3. Todos los empleados entrevistados se mostraron interesados y disponibles en participar en las iniciativas de seguridad de la información.
4. La mayoría de los empleados no saben cómo funcionan, ni cuales son las principales estrategias de ataques informáticos.
5. Para la mayoría de los empleados el acceso a su computadora representa un riesgo solamente para la información que está almacenada en su interno.
6. La mayoría de los empleados no conocen y, de consecuencia, no respetan la política de seguridad.
7. La mayoría de los entrevistados usa la misma clave para todo.
8. La mayoría de los entrevistados piensa que la competencia sería el principal beneficiario en obtener la información que la agencia maneja o posee.
9. La mitad de los entrevistados no suele bloquear su computadora del trabajo cuando abandona su estación de trabajo y en los peores de los casos no suele tener clave.
10. La mayoría de entrevistados no considera importante protegerse porque piensan que no son targets valiosos o que podrían ser víctimas de ataques informáticos.

4.4 Comparación y análisis de los resultados

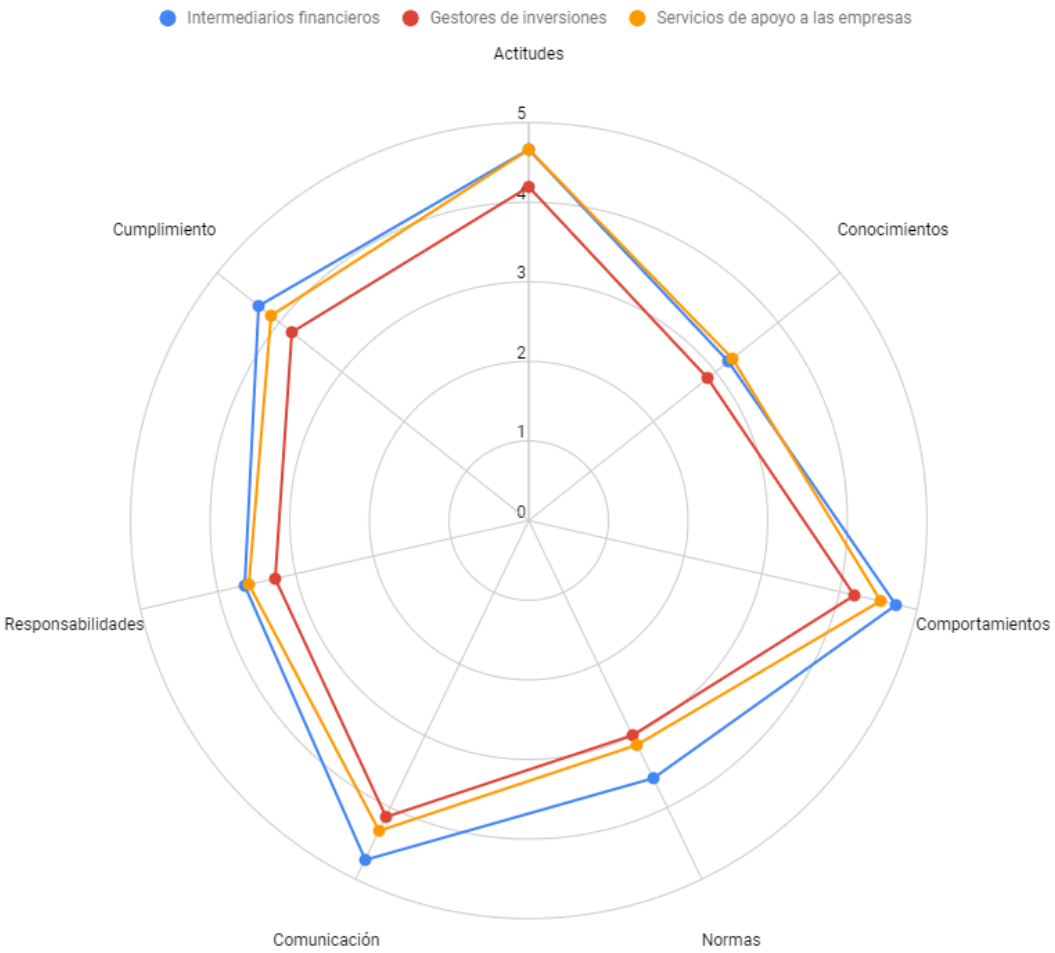
La información que se ha recolectado durante las entrevistas nos ha permitido tomar una instantánea del estado de la cultura de la ciberseguridad de los empleados. En particular vamos a analizar dos aspectos claves de esta instantánea:

- La cultura de ciberseguridad.
- El valor de la información.

4.4.1 Análisis de la cultura de ciberseguridad

Gracias a los datos recolectados en el estudio CLTRe podemos comparar nuestra instantánea con sus modelos. De hecho, los investigadores de CLTRe han organizado la información según áreas y funciones de negocio. Esto para poder evidenciar las diferencias en las necesidades culturales en la seguridad de la información según el rubro de pertenencia y las funciones que la empresa realiza.

Img. 4.1



En particular la agencia que hemos analizado pertenece al rubro de “Servicios de apoyo a las empresas”.

Img. 4.2

Como podemos observar en el grafico Img. 4.2, la empresa que hemos examinado presenta una puntuación anómala para su categoría en los indicadores de Comportamientos, Comunicación y Cumplimiento. Vemos como en nuestro caso la cultura de seguridad no es madura ni conforme a los modelos observados por CLTRe. Estas grandes diferencias se ven reflejadas en los hallazgos 4 y 5 por los indicadores Comportamientos y Comunicación, y los hallazgos 2 y 6 para el indicador Cumplimiento.

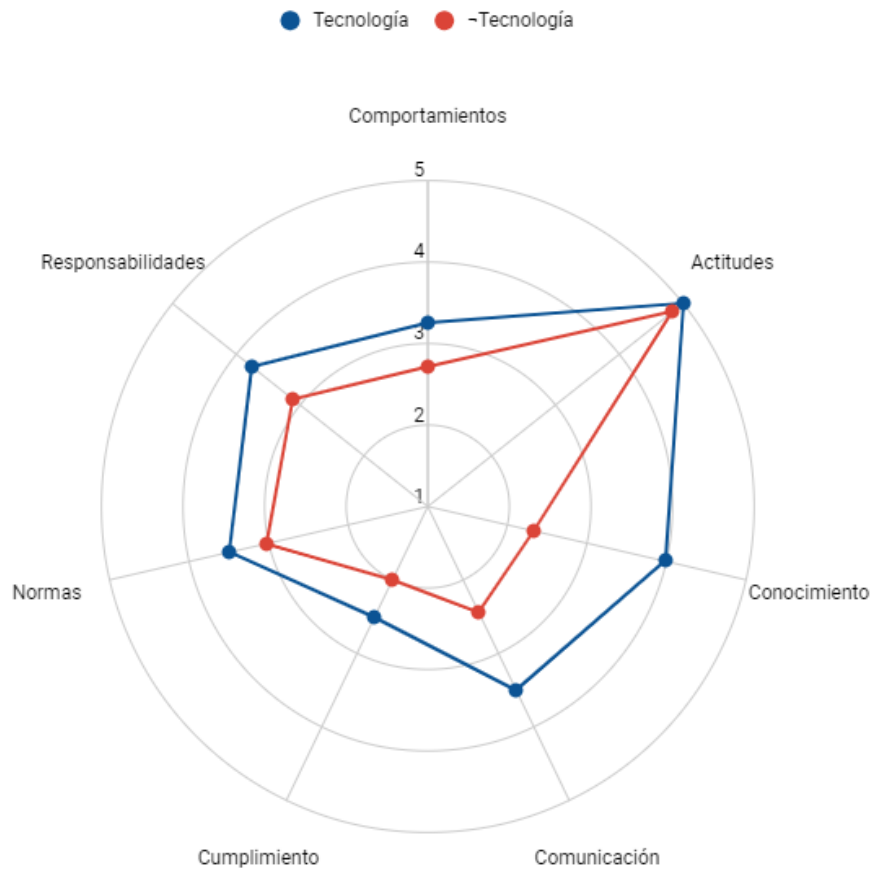
Analizamos ahora más detenidamente cada indicador para poder interpretar su puntuación:

1. **Actitudes**:
   Es el indicador con la puntuación más alta entre todos. Respecta el modelo observado por los investigadores CLTRe. Podemos interpretar la elevada puntación como una

buena señal de madurez para la cultura de la seguridad acerca de este indicador. En general al instaurar una estrategia de seguridad de la información, en una organización se busca una ventana de oportunidad. Se trata de un evento o una situación particular que permite impulsar el desarrollo de la estrategia. De hecho, este indicador es muy importante para la fase de implementación si se quiere establecer una nueva estrategia de seguridad de la información, o simplemente proponer una nueva iniciativa. Podemos afirmar que una puntuación tan alta para el indicador Actitudes representa una óptima ventana de oportunidad para el desarrollo de nuestra estrategia.

2. **Conocimientos**:
El indicador en promedio no alcanza el nivel 3, que según nuestra escala de evaluación cualitativa es el umbral mínimo para que no sea considerado un problema. Analizando las mediciones agrupadas por área, vemos que el área de tecnología alcanza un nivel satisfactorio, mientras el resto de los entrevistados permanece en el nivel de elevado peligro.

Img. 4.3



La diferencia es peligrosa porque impide una comunicación fluida y eficaz entre las distintas áreas de la agencia, ralentizando los procesos de interacción y poniendo en peligro su seguridad: no conociendo los peligros existentes no es posible tomar las contramedidas necesarias para contrastarlos.

3. **Comportamientos**:
El indicador difiere peligrosamente de la del modelo observado por CLTRe. Una gran parte de los entrevistados demuestra que no se hacen cargo de cuidar sus contraseñas, no utilizan sistemas de copia de seguridad seguros o fiables, no protegen sus dispositivos ni los archivos corporativos almacenados en ellos. CLTRe afirma que este tipo de comportamiento plantea un serio riesgo a la organización, por tanto, aunque en adoptar dicho comportamiento es sólo una minoría, la puntuación de este indicador representa un grave riesgo para la organización.

Aquí también podemos ver que en general el área de tecnología se comporta mejor que el resto de la organización. También hay que señalar que, contrariamente a lo que se podría pensar un alto indicador de conocimientos no corresponde a un alto indicador de comportamientos. De hecho, CLTRe encuentra que, a pesar de que los trabajadores son conscientes de los riesgos que corren, todavía adoptan comportamientos peligrosos. De ahí la necesidad de actuar sobre el aspecto cultural en lugar de la formación técnica del personal.

4. **Comunicación**:
Como vemos en el gráfico Img. 4.2 este indicador también tiene un valor poco tranquilizador, en promedio, de hecho, no alcanza el nivel 3. Difiere por casi dos puntos del modelo observado por los investigadores de CLTRe y presenta la misma peculiaridad del indicador Conocimientos: sólo las puntuaciones de los entrevistados pertenecientes al área de tecnología superan el umbral de peligrosidad. Esto significa que en la organización la comunicación de temas relacionados con la seguridad informática es escasa o ausente.

Esto conlleva riesgos muy serios como:

- La incapacidad de reconocer y, por tanto, de comunicar un problema.
- Los trabajadores no sienten la necesidad de iniciativas de seguridad de la información, porque no es un tema de conversación entre los trabajadores.
- Los trabajadores no tienen las habilidades necesarias para establecer una cultura de autoevaluación construida sobre la retroalimentación recíproca de los propios trabajadores.

5. **Normas**:
A pesar de que el nivel medio de este indicador se acerque al modelo observado por el CLTRe, no alcanza el umbral de la peligrosidad. Este indicador tiene una fuerte influencia en los de Conocimientos y Comportamientos, ya que es el aspecto cultural que guía a los trabajadores en la evaluación de lo que es normal o importante y lo que parece extraño en el contexto organizacional. De hecho, se ha constatado que existe una fuerte dificultad para evaluar tales acciones peligrosas desde el punto de vista de la seguridad, si no en los casos en que es difícil acogerse al sentido común. Esto es probablemente debido a la falta de conocimiento de cuáles son las amenazas y las metodologías

utilizadas por aquellos que intentan aprovecharse de la organización.

6. **Responsabilidades**:
La puntuación de este indicador difiere poco menos de medio punto del modelo observado por CLTRe. Se coloca exactamente en el umbral entre problemático e inseguro con una puntuación media de 3. Esto se debe al hecho de que los roles de responsabilidad no están bien definidos dentro de la agencia. Además, no existe un sistema de gestión de responsabilidad para la información que los empleados manejan en su día a día. Estos factores conducen inevitablemente a una confusión de roles y responsabilidades, y sobre todo a su percepción distorsionada por los trabajadores. También en este caso el área de tecnología tiene más conciencia de las responsabilidades relacionadas con el tratamiento de la información sensible que el resto de la agencia. A excepción de muy pocos casos, este último cree que la responsabilidad por el uso que se hace de la información corporativa es sólo del área de tecnología.

7. **Cumplimiento**:
Es el indicador con la puntuación más baja, se posiciona en el área de alto peligro, con más de dos puntos menos respecto al modelo observado por CLTRe. Una nota discordante de la cultura de seguridad de la agencia que presenta un gran factor de riesgo. De hecho, como no hay ninguna política de seguridad compartida y conocida por todos los trabajadores de la organización, fue difícil medir este indicador. La mayoría de los entrevistados ignoran la existencia de documentos relativos a la confidencialidad, integridad y responsabilidad legal de la información que se produce y gestiona dentro de la agencia. No hay una cultura fuerte que pueda transmitir la importancia de este aspecto de la seguridad informática. Siendo más complicados de explicar y de hacer asimilar a los trabajadores, la necesidad de poseer una política de seguridad se ve más que nada como una limitación que una protección.

4.4.2 Análisis del valor de la información

Además de analizar la cultura de la seguridad informática, se quiere entender cuál es el valor que los entrevistados adjuntan a la información que manejan. En un mundo donde la información se ha convertido en uno de los principales recursos para una empresa, pensamos que es esencial que los trabajadores puedan entender su valor para facilitar la toma de decisiones. Se ha analizado la percepción del valor de la información examinándolo en 3 dimensiones:

- Valor intrínseco y económico de la información:
  ¿El empleado es capaz de reconocer cuál es la información que procesa y produce para la agencia?
- Impacto de la pérdida de información:
  ¿El empleado es capaz de cuantificar la pérdida económica por robo o destrucción de la información que procesa y produce para la agencia?
- Confidencialidad de la información:
  ¿El empleado es capaz de distinguir la información sensible y confidencial de la agencia?

Tomando en cuenta las 3 dimensiones analizadas para la información que cada empleado maneja: Valor, Impacto y Confidencialidad, se nota una incongruencia lógica. La mayoría de los empleados no atribuye mucho Valor a la información que manejan ni le

prestan mucho cuidado a nivel de Confidencialidad, pero sí consideran que el Impacto de su destrucción o pérdida sería elevado/importante. No hay un marco normativo que los obligue a proteger la información que manejan, ni si fomentan buenas prácticas de ciberseguridad al interno de la organización. Los empleados no conocen los riesgos que están expuestos no protegiendo la información de la agencia, y esta última no los capacita para que puedan tomar conciencia de la importancia de protegerla.

Esto se puede reconducir a la falta de Cumplimiento y Comunicación, y también al hecho de que muy pocos de los empleados entrevistados saben cómo se lleva a cabo un ataque informático, y cuáles son sus consecuencias.
A eso se suma la dificultad en reconocer las Responsabilidades del rol que cada trabajador ocupa dentro de la organización.

Como hemos visto, los empleados entrevistados están predispuestos a participar activamente en las iniciativas de seguridad de la información. Esto, junto a la necesidad de proteger la información que manejan y consideran muy valiosa para la organización y sus clientes, constituye un punto de activación óptimo para el desarrollo de una estrategia de seguridad de la información. El grupo de seguridad tomando en cuenta esta ventana de oportunidad, quiere llevar a cabo los cuatro objetivos a través la implementación de controles de seguridad. Los controles propuestos han sido pensados para abordar los principales hallazgos de las entrevistas. La estrategia estará basada en controles de seguridad a la vanguardia presentados en el moderno Cybersecurity Framework de NIST (National Institute of Standards and Technology).

5. Fase de Planificación

Una vez que hemos analizado todos los aspectos culturales tenemos que considerar los hallazgos principales para poder diseñar y sucesivamente desarrollar una correcta estrategia de seguridad de la información. Hemos analizado singularmente cada indicador para poder ver cuáles podrían ser las causas y las consecuencias de su puntación global.

Gracias a este análisis hemos podido aislar los aspectos principales de cada indicador cultural, permitiéndonos de identificar cual macrobjetivo afectan en particular. Principalmente, lo que queremos obtener es un mapeo completo de las funciones principales de Framework de referencia con los macrobjetivos de nuestra estrategia. Para realizar este mapeo seleccionaremos los controles propuestos por el Cybersecurity Framework que abarcan las funciones necesarias para cumplir el macrobjetivo correspondiente.

Para poder seleccionar los controles en la manera más adecuada, hemos recurrido a la construcción de un DAFO. De esta manera hemos dado una visibilidad mayor a los hallazgos de nuestro análisis etiquetándolos como:

- Debilidades
- Amenazas
- Fortalezas
- Oportunidades

Podemos entonces aprovechar esta categorización para decidir con mayor agilidad los controles más adecuados en función de:

- Las debilidades principales que hemos evidenciado gracias a las puntuaciones de los indicadores culturales y a las entrevistas realizadas en la fase de investigación.
- Las amenazas impulsadas por entorno empresarial moderno, los riesgos de los ciberataques y de las multas para no respectar los marcos normativos legales y regulatorios vigentes.
- Las fortalezas representadas por las más altas puntuaciones de los indicadores de cultura de ciberseguridad y por los principales hallazgos de las entrevistas.
- Las Oportunidades generadas por el entorno empresarial moderno y por el indicador de Actitudes.

Para la realización del DAFO hemos reorganizado los hallazgos de la fase de Análisis y durante una dinámica grupal entre el grupo de seguridad de la organización, los hemos etiquetados.

Aquí podemos ver el grafico generado:

Debilidades: • No existe una política de seguridad • Escaso conocimiento de los temas relacionados a la seguridad de la información • Bajo interés por la seguridad de la información que los empleados manejan • Los roles y las responsabilidades acerca de la seguridad de la información no han sido establecidos.	**Amenazas**: • La competencia suele preocuparse más por la seguridad de la información, y esto podría resultar en que los clientes los vean como mejor opción que nuestra agencia. • No cumplir con el marco normativo vigente puede conllevar a multas muy elevadas, y de consecuencia a dañar la reputación de la agencia. • Número creciente de incidentes de seguridad que han afectado el negocio
Fortalezas: • En general, los trabajadores tienen una buena actitud hacia el desarrollo de una estrategia de seguridad. • El equipo de tecnología posee buenos conocimientos de seguridad de la información. • Flexibilidad: Equipo joven que ha interiorizado metodologías ágiles de gestión del cambio.	**Oportunidades**: • Arrancar desde cero el desarrollo de una estrategia de seguridad • Ventana de buena actitud hacia las iniciativas de seguridad de la información. • Ventana de número creciente de incidentes de seguridad. • Aprovechar los conocimientos del área de tecnología para el desarrollo de la estrategia.

Siendo el Framework tecnológicamente neutro podemos seleccionar los controles independientemente de los detalles de implementación. Será el objetivo de la fase de Implementación bajar en los detalles más técnicos de implementación. Por el momento nos limitaremos en considerar nuestros 4 macrobjetivos como directrices que nos ayuden en seleccionar los controles propuestos por el Framework. Eso nos resulta muy cómodo en esta fase preliminar ya que podemos concentrarnos solamente en los hallazgos evidenciados en la fase de Análisis.

Los controles se desglosan por cada objetivo según las funciones del Cybersecurity Framework:

- Identify: Cumplen esta función los controles de seguridad que nos ayudan en identificar problemas en la estructura de nuestra organización, definir infraestructuras robustas y

de fácil gestión, mejorar las existentes y finalmente entender cuáles son los procesos clave para nuestra organización.

- Protect: Cumplen esta función los controles de seguridad que nos permiten proteger nuestros activos, garantizar un nivel de protección adecuado a la información que nuestros empleados manejan, así como asegurar que el acceso a dicha información solo sea garantizado a quien tiene derecho.
- Detect: Cumplen esta función los controles de seguridad que nos permiten detectar eventos anómalos en nuestros procesos: intentos de ataques, incidentes de seguridad, robos de datos, etc. Así como asegurar que los responsables sean identificados.
- Respond: Cumplen esta función los controles de seguridad que nos ayudan en definir los procesos para poder responder a un incidente de seguridad, a una anomalía o un intento de ataque.
- Recover: Cumplen esta función los controles de seguridad que nos ayudan en definir las políticas de continuidad de negocio y los procesos que nos permiten lograr la recuperación de nuestras actividades después de un incidente de seguridad.

La idea es que cada macrobjetivo cumpla una o más funciones para que la estrategia propuesta pueda satisfacer el Framework de referencia. En base a los controles que caracterizan las funciones del Framework podemos mapear estas últimas con los objetivos de nuestra estrategia de seguridad de la información. En particular el mapeado de los objetivos de la estrategia con las funciones del Framework es la siguiente:

- Organización estructural que abarca todas las 5 funciones del Framework
- Cultura de trabajo que abarca las funciones Protect y Detect
- Concienciación de seguridad que abarca las funciones Protect, Detect y Respond
- Gobierno de ciberseguridad que abarca las funciones Identify, Detect y Recover

Logrando estos 4 objetivos vamos a cubrir cada función del cybersecurity framework propuesto da NIST, que se ha tomado en cuenta para seleccionar los controles.

Vamos a presentar los macros objetivos con los correspondientes controles seleccionados agrupados por funciones del Framework:

Organización Estructural

Este macroobjetivo juega un rol principal en la estrategia de seguridad para la nuestra agencia. Su realización permite cubrir todas las funciones del Cybersecurity Framework encontrando un equilibrio entre las medidas de seguridad y las necesidades del negocio.

A través de un análisis profundo de los procesos de la agencia, de sus activos y de las responsabilidades del personal, busca definir los roles clave de la organización para proteger sus activos y garantizar el correcto funcionamiento de sus procesos.

A través de la reorganización de la estructura organizativa de la agencia busca administrar los riesgos de manera eficiente mitigándolos y reduciendo su posible impacto.
Este macroobjetivo a través de los controles propuestos trata de mejorar los aspectos evidenciados por los indicadores de Cumplimientos, Normas, Responsabilidades, Comunicaciones y Comportamientos. También por el aspecto de la cultura de la seguridad vemos como este macroobjetivo es muy relevante para la estrategia de seguridad.

Sucesivamente proporcionamos el listado de las funciones del Cybersecurity Framework que este objetivo cubre:

Identify:

Gestión de los Assets: Establecer roles y responsabilidades en la ciberseguridad para la entera workforce de la agencia.
Gobierno: Coordinar y establecer los roles de ciberseguridad en la organización.
Estrategia de gestión de riesgos: Definición de un proceso de gestión de riesgo y de una tolerancia al riesgo.

Protect:

Gestión de identidad, y control de autenticación y acceso:
incorporación del principio del mínimo privilegio para los accesos.

Detect:

Proceso de detección: Definición de roles y responsabilidades para garantizar la rendición de cuentas.

Respond:

Comunicaciones: El personal conoce su roles y operaciones cuando es necesaria una acción de respuesta a un incidente.

Recover:

Comunicaciones: Gestión de las relaciones públicas para restaurar las actividades coordinando con los agentes internos y externos

Cultura de Trabajo

Este macroobjetivo remarca la importancia de la creación de una cultura de ciberseguridad que se adapte al mundo laboral moderno. Controlar los activos se ha vuelto muy difícil ahora que la información esta compartida en la red y se puede acceder por los dispositivos privados de los trabajadores. Para los empleados también es complicado manejar esta información sensible de forma responsable.

Este objetivo busca construir una cultura que tenga un enfoque hacia el patrón CAMS (Cloud, Analytics, Mobile, Social)[18] para proporcionar a la empresa y a los trabajadores las herramientas para gestionar la información de forma responsable y segura.
En particular, busca mejorar los aspectos culturales evidenciados por los indicadores de Comportamientos, Normas, Responsabilidades y Cumplimiento.

Sucesivamente proporcionamos el listado de las funciones del Cybersecurity Framework que este objetivo cubre:

Protect:

Gestión de identidad, y control de autenticación y acceso: Proteger y gestionar el acceso físico a los activos de la agencia.
Gestionar el acceso remoto a los activos de la agencia.
Data security: Proteger los datos en reposo de los activos de la agencia.
Procesos y procedimientos de protección de la información:
Efectuar, monitorizar y testear *backups* de la información.

Protección tecnológica: Incorporar el principio de la mínima funcionalidad en la configuración de los sistemas para garantizar solamente las funcionalidades necesarias.

Detect:

Anomalías y Eventos: Establecer un umbral de alerta para los incidentes de seguridad.
Proceso de detección: Establecer y testear un proceso de detección de los eventos, para que los trabajadores puedan detectar un evento de seguridad.

Concienciación de ciberseguridad

Este macrobjetivo trata de concienciar dinámicamente las áreas de la empresa creando programas distintos para cada una de ellas. Esto resultaría en generar mayor interés e implicación del empleado en el programa de concienciación, aumentando eficacia y eficiencia del proceso de concienciación.
Este objetivo busca mejorar los aspectos culturales evidenciados por los indicadores de Conocimientos, Comportamientos, Normas, Responsabilidades y Comunicaciones. Los controles propuestos para este objetivo buscan, sobre todo, capacitar el personal de la agencia para garantizar la seguridad en el funcionamiento de sus procesos.

Sucesivamente proporcionamos el listado de las funciones del Cybersecurity Framework que este objetivo cubre:

Protect:

Concienciación y capacitación: Capacitar todos los trabajadores sobre su roles y responsabilidades.
Capacitar a los usuarios con privilegios de acceso.

Detect:

Anomalías y Eventos: Capacitar a las áreas de cybersecurity sobre eventos de seguridad y anomalías.

Respond:

Comunicación, Análisis y Mitigación: Capacitar las áreas de cybersecurity sobre cómo reportar, analizar y mitigar un evento de seguridad.

Gobierno de ciberseguridad

Este macroobjetivo busca administrar los recursos de seguridad de manera que la infraestructura generada sea eficaz y eficiente, y funcione según el marco regulatorio vigente. Además, busca monitorizar todos los procesos de la infraestructura de seguridad para garantizar que se alcancen los objetivos de la agencia, que se cumpla el marco regulatorio y legal, y que todas las medidas de seguridad implementadas para lograr los demás objetivos operen como planteado.
Este objetivo busca mejorar los aspectos culturales evidenciados por el indicador de Cumplimiento, Normas y Comportamientos.

Sucesivamente proporcionamos el listado de las funciones del Cybersecurity Framework que este objetivo cubre:

Identify:

Gobierno: Aclarar y gestionar los requerimientos legales y regulatorios acerca de la seguridad de la información, privacidad y confidencialidad.
Entorno Business: Entender la misión y los objetivos de la agencia para poder establecer roles y responsabilidades en la cybersecurity y las decisiones de gestión de riesgos.

Detect:

Monitorización continua de la seguridad: Monitorizar los servicios y procesos internos y externos de la agencia para detectar potenciales eventos de ciberseguridad.

Recover:

Mejoras y Comunicación: Incorporar en los planes de recuperación con las lecciones aprendidas por eventos pasados.
Comunicar las acciones de recuperación cumplidas a los equipos de gestión y ejecutivos.

Hemos visto como los controles cubren todas las funciones del Cybersecurity Framework NIST, proporcionando soluciones a los principales hallazgos encontrados en la fase de Análisis, y logrando los 4 macrobjetivos que hemos planteado para nuestra estrategia de seguridad de la información.
Los controles propuestos no pueden, solos, lograr nuestros objetivos. Necesitamos proporcionar iniciativas que implementen dichos controles, logrando una o más de las funciones del Framework, para finalmente cumplir nuestros objetivos y poner en marcha la estrategia de seguridad planteada. El proceso de Implementación se enfocará en este aspecto, tratando de hacer realidad los controles planteados.

6. Fase de Implementación

Implementaremos la estrategia de seguridad de la información considerando los 4 objetivos como líneas estratégicas. Para cada uno de ellos vamos a esbozar los objetivos estratégicos basados en las funciones y controles del Cybersecurity Framework que propusimos en la fase de Planificación.

Con el fin de alcanzar estos objetivos estratégicos, se propondrán iniciativas concretas para intentar implementar los controles previstos. Este tipo de Iniciativas presentan características peculiares tales que respecten la fórmula SMART [19].

La fórmula SMART se compone de 5 características:

- S: Specific (Especifico)
- M: Measurable (Medible)
- A: Achievable (Realizable)
- R: Realistic (Realístico)
- T: Timed (Cronometrado)

La fórmula nos obliga a ser tan específico como podemos, añadiendo los detalles y el enfoque necesarios a la iniciativa. Al ser medible, una iniciativa SMART nos permite saber cuándo hemos alcanzado el objetivo. Ser realizable significa que disponemos de los recursos para poder hacer lo que hemos establecido. Realístico porque que nos hemos fijado para hacer algo real; esto no es algo abstracto e impreciso. Por último, un objetivo SMART debe tener un plazo claramente definido, para que nos ayude a planificarlo.

Una iniciativa puede abarcar una o más de las funciones del marco de ciberseguridad del NIST. En particular, las iniciativas propuestas deben garantizar la cobertura total de los controles propuestos en la etapa de Planificación. Antes de implementar las iniciativas de seguridad propuestas, estas pasaran a través de un proceso de priorización.

La priorización de las iniciativas se logrará a través de una matriz de coste-beneficio. Con el fin de medir el beneficio de la iniciativa, nos basaremos en el número de objetivos estratégicos que pretende completar. Cuanto mayor sea el número de objetivos estratégicos involucrados en el curso de la iniciativa, mayor será el beneficio.

Para simplificar no hemos dado un peso a los objetivos estratégicos, lo que significa que no hay un objetivo más importante que otro. Para ciertas estrategias podría ser útil asignar un peso a los objetivos para hacer más eficaz la priorización.

6.1 Iniciativas Propuestas

Vamos a presentar las iniciativas propuestas con las relativas propiedades y priorización. Por cada iniciativa propuesta se listan los objetivos estratégicos que cubre y los correspondientes controles del Cybersecurity Framework agrupados por funciones. El número de objetivos

estratégicos que la iniciativa va a cubrir influenciaran el beneficio aportado. Cada iniciativa tiene como objetivo la puesta en marcha de los proyectos o servicios que la caracterizan. Los proyectos o servicios afectarán el coste de la iniciativa.

1) Establecer los roles de ciberseguridad y responsabilidad al interno de la organización:

Objetivos Estratégicos:

Organización Estructural:

- Identify: Gobierno, Gestión de los activos
- Detect: Proceso de detección

Concienciación de Ciberseguridad:

- Protect: Concienciación y Capacitación

Gobierno de seguridad:

- Identify: Gobierno, Entorno Business

Beneficio: 6

Proyectos o Servicios:

1. Establecer oficialmente un sistema organizacional de ciberseguridad con las relativas responsabilidades definidas y los roles asignados.
2. Curso de concienciación sobre las responsabilidades de los trabajadores
3. Curso de concienciación sobre las obligaciones legales de los trabajadores

Métricas:

- % Tiempo invertido / % Tiempo estimado

- % Trabajadores en el área de ciberseguridad que tienen oficialmente un rol de responsabilidad asignado.

- % Participantes para los cursos de concienciación. / % De inscritos

- # Horas por semana que los inscritos participan a los cursos de concienciación.

- Promedio de notas del curso de concienciación.

- Promedio de satisfacción con los cursos de concienciación.

2) Datos seguros:

Objetivos Estratégicos:

Organización Estructural:

- Protect: Gestión de identidad, y control de autenticación y acceso

Cultura de Trabajo:

- Protect: Gestión de identidad, y control de autenticación y acceso, Data security, Procesos y procedimientos de protección de la información, Protección tecnológica

Concienciación de Ciberseguridad:

- Protect: Concienciación y capacitación

Beneficio: 6

Proyectos y Servicios:

1. Implementación de sistema de acceso a las oficinas vía *badge*
2. Instalación de servicio de cifrado de disco en las computadoras de la agencia
3. Instalación de servicio de *backup* automático en las computadoras de la agencia
4. Instalación de servicio de acceso basado en roles para los usuarios de las computadoras de la agencia.
5. Curso de capacitación sobre riesgos y responsabilidades del rol administrador de los dispositivos de la agencia

Métricas:

- % Tiempo invertido / % Tiempo estimado
- Promedio de satisfacción con el uso del badge para el acceso a las oficinas
- # Backups efectuados / # Total de computadoras de la agencia
- # Discos cifrados / # Discos de las computadoras de la agencia
- # Computadoras con servicio de acceso basado en roles / # Total de computadoras de la agencia
- % Participantes para los cursos de capacitación. / % De inscritos
- # Horas por semana que los inscritos participan a los cursos de capacitación.
- Promedio de notas del curso de capacitación.
- Promedio de satisfacción con los cursos de capacitación.

3) Establecer una estrategia de gestión de riesgos:

Objetivos Estratégicos:

Organización Estructural:

- Identify: Estrategia de gestión de riesgos

Gobierno de Seguridad:

- Identify: Entorno Business
- Recover: Mejoras y Comunicación

Beneficio: 6

Proyectos o Servicios:

1. Realizar un Análisis de Riesgos que comprende personas, procesos y tecnologías
2. Establecer una estrategia de Gestión de Riesgos en base al Análisis de Riesgos
3. Establecer un nivel de tolerancia basado en la estrategia de Gestión de Riesgos.
4. Establecer un proceso de mejora continua de la estrategia de Gestión de Riesgos
5. Proporcionar un canal de comunicación para compartir informaciones de las políticas y estrategias de gestión de riesgos a los equipos de gestión de proyectos y a los ejecutivos

Métricas:

- % Tiempo invertido / % Tiempo estimado
- % Activos de la agencia analizados / % Activos totales de la agencia
- # Riesgos gestionados / # Riesgos identificados
- Promedio de satisfacción con la estrategia de gestión de riesgos entre los empleados.
- # Procesos con riesgo superior al umbral prefijado / # Procesos con riesgo inferior al umbral prefijado
- # Trabajadores que usan el canal de comunicación para compartir informaciones de las políticas y estrategias de gestión de riesgos / # Trabajadores en los equipos de gestión de proyectos y ejecutivos

4) Establecer una estrategia de respuestas a incidentes de seguridad:

Objetivos Estratégicos:

Organización Estructural:

- Respond: Comunicaciones

Cultura de Trabajo:

- Detect: Anomalías y Eventos, Proceso de detección

Concienciación de Seguridad:

- Detect: Anomalías y Eventos
- Respond: Comunicación, Análisis y Mitigación:

Gobierno de la Seguridad:

- Detect: Monitorización continua de la seguridad

Beneficio: 7

Proyectos o Servicios:

1. Definir las operaciones necesarias y los roles del personal de seguridad en caso de incidente de seguridad.
2. Definir el umbral de alerta de un incidente de seguridad.
3. Instalar un sistema IDS en Red para poder notificar el personal de seguridad de eventos que superan el umbral de alerta prefijado.
4. Asignar recursos del personal de seguridad a la manutención y monitorización del sistema IDS.
5. Capacitar el personal de seguridad sobre los roles y operaciones necesarias en caso de incidente de seguridad.
6. Capacitar todo el personal de la agencia sobre como comunicar y detectar un incidente de seguridad.

Métricas:

- % Tiempo invertido / % Tiempo estimado
- % Trabajadores en el área de ciberseguridad que tienen oficialmente un rol de responsabilidad asignado.
- % Recursos asignados a la manutención del IDS / % Recursos necesarios a la manutención del IDS
- # Intentos de intrusión detectados por el IDS / # Intentos de intrusión totales
- % Participantes para los cursos de capacitación. / % De inscritos
- # Horas por semana que los inscritos participan a los cursos de capacitación.
- Promedio de notas del curso de capacitación.
- Promedio de satisfacción con los cursos de capacitación.

5) Establecer un proceso de gestión del riesgo reputacional:

Objetivos Estratégicos:

Organización Estructural:

- Recover: Comunicación

Beneficio: 1

Proyectos y Servicios:

1. Designar los responsables de las relaciones públicas
2. Capacitar los responsables de las relaciones públicas para gestionar el riesgo reputacional de un incidente de seguridad

Métricas:

- % Tiempo invertido / % Tiempo estimado
- # Responsables de las relaciones publicas designados / # Responsables de las relaciones publicas planteados
- # Riesgos reputacionales gestionados / # Riesgos reputacionales individuados
- # Eventos de seguridad que afectan la reputación gestionados por el equipo de relaciones públicas / # Eventos de seguridad totales que afectan la reputación
- % Participantes para los cursos de capacitación. / % De inscritos
- # Horas por semana que los inscritos participan a los cursos de capacitación.
- Promedio de notas del curso de capacitación.
- Promedio de satisfacción con los cursos de capacitación.

6.2 Presupuesto

Ahora vamos a analizar el coste de las iniciativas de seguridad propuestas para poder considerarlo al momento de calcular su priorización. El análisis de los costes nos permite también determinar la viabilidad de cada iniciativa en términos estrictamente económicos. Generalmente en pequeñas empresas no se dispone de un presupuesto elevado por la seguridad de la información, por ende, es fundamental aprovechar a lo mejor cada mínima inversión. Además, este análisis nos ayuda en determinar el factor A (Achievable) y R (Realistic) que queremos respectar para obtener objetivos SMART.

Presentaremos los costes de las iniciativas en una tabla que nos permita tener en cuenta costes totales y unitarios por cada proyecto/servicio de las iniciativas propuestas.

	Unidad	Cantidad	Coste unitario en USD $	Coste total en USD $
Iniciativa 1: Establecer roles de ciberseguridad y responsabilidad interna				**8800**
Establecimiento de roles	# horas trabajadas	8	30	240
Curso de concienciación sobre las responsabilidades	# personas	107	20	2140
Curso de concienciación sobre las obligaciones legales	# personas	107	60	6420

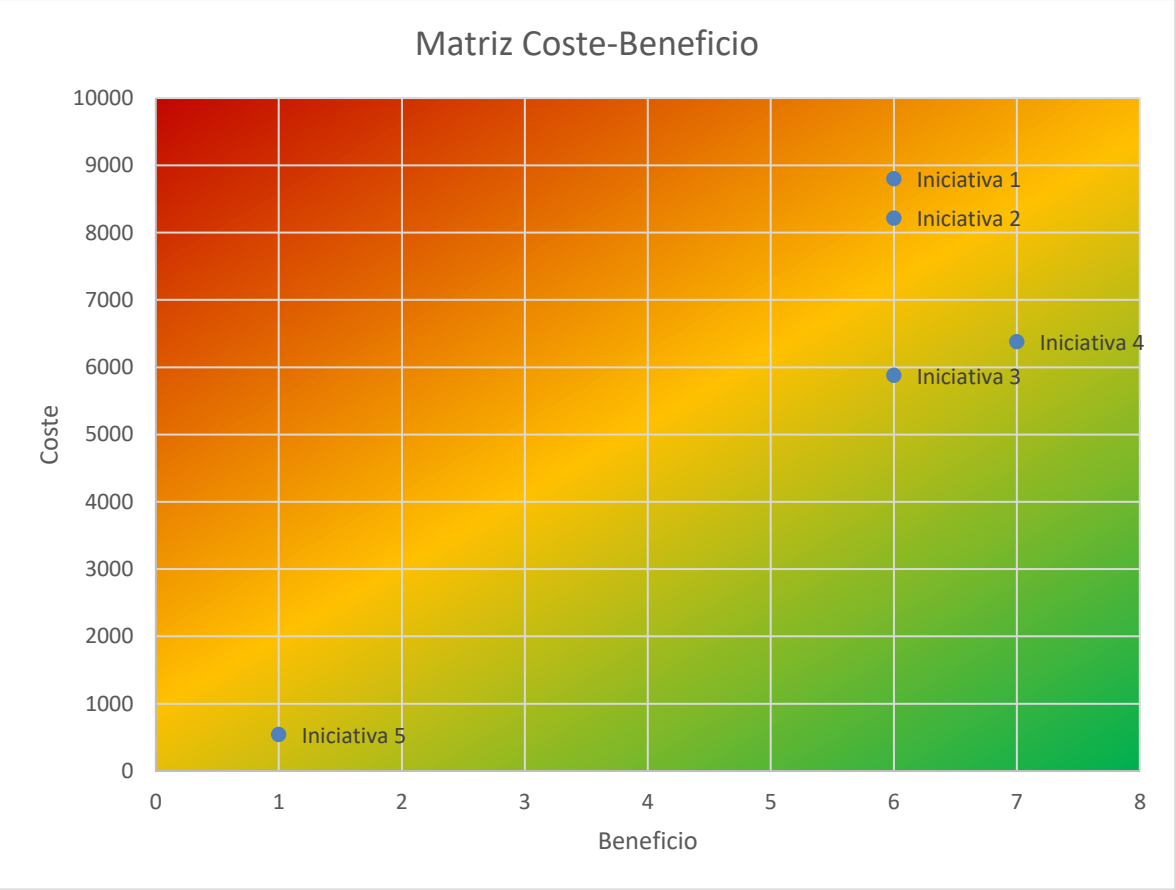
Iniciativa 2: Datos seguros				**7015**
Sistema de acceso con badge	# sistema	1	1000	1000
Badge	# personas	107	5	535
Configuración backup, cifrado y RBAC	# horas trabajadas	80	15	1200
Curso de capacitación sobre riesgos y responsabilidades	# personas	107	40	4280
Iniciativa 3: Establecer una estrategia de gestión de riesgos				**5880**
Análisis de riesgos	# horas trabajadas	240	15	3600
Estrategia de gestión de riesgos	# horas trabajadas	120	15	1800
Implementación de un canal de comunicación	# horas trabajadas	16	30	480
Iniciativa 4: Establecer una estrategia de respuestas a incidentes de seguridad				**6380**
Establecimiento de roles	# horas trabajadas	8	30	240
NIDS	# servidores	3	500	1500
Configuración del NIDS	# horas trabajadas	24	15	360
Curso de capacitación sobre roles y operaciones	# horas trabajadas	107	20	2140
Curso de capacitación sobre como comunicar y detectar un incidente	# horas trabajadas	107	20	2140
Iniciativa 5: Establecer un proceso de gestión del riesgo reputacional				**540**
Asignación de los responsables de RRPP	# horas trabajadas	8	30	240
Curso de capacitación para los responsables de RRPP	# de personas	3	100	300
			TOTAL	**28615**

En total el presupuesto para la implementación completa de las iniciativas de seguridad propuestas es 28615 USD$. Este monto es provisorio ya que ahora las iniciativas pasaran por un proceso de priorización que podría llevar hasta a descartar algunas de ellas.

6.3 Priorización de las iniciativas

Establecidas las iniciativas y sus propiedades, hay que priorizar su implementación. Por cada iniciativa tenemos dos indicadores que nos ayudaran en esto proceso: el coste y el beneficio. En particular gracias a una matriz de coste-beneficio cada iniciativa tendrá una puntuación que será más alta cuanto más alto será la proporción entre el coste y el beneficio.

Img 6.1



Como podemos observar en la gráfica Img. 6.1 la priorización resultante de la matriz coste-beneficio es:

1) Establecer una estrategia de respuestas a incidentes de seguridad
2) Establecer una estrategia de gestión de riesgos
3) Establecer un proceso de gestión del riesgo reputacional
4) Datos seguros
5) Establecer los roles de ciberseguridad y responsabilidad al interno de la organización

Esto será el orden de implementación mejor para optimizar los tiempos y los recursos de la agencia al momento de desarrollar la estrategia de seguridad propuesta.

6.4 Medición y Proceso de Mejora Continua

Cada iniciativa propuesta debe ser medible para que disponga de las propiedades SMART. Su mediación es fundamental para entender su efectividad y eficiencia. Para hacer esto posible será necesario formular una o más métricas para cada iniciativa de seguridad. Estas métricas nos ayudarán a entender si la iniciativa funciona, ya sea que tengamos que cambiarla un poco o totalmente. En general, el objetivo de una iniciativa de seguridad es lograr una transformación dentro de nuestra organización.

Para generar una métrica, es necesario entender el estado actual, definido por la ISO 27000 *"as is"* o como es, y lo que queremos lograr, llamado *"to be"* o como debe ser. De esta manera podemos entonces medir la transformación y entender cuando ha tenido éxito o no. Las métricas nos permiten que está sucediendo durante el periodo de desarrollo de nuestras iniciativas, permitiéndonos de conocer su estado actual. A su vez nos permiten medir el avance del macroobjetivo correspondiente, haciendo más visibles aspectos de las relaciones entre los objetivos y las funciones que cumplen, o deberían cumplir. Por otro lado, promueven la mejora de los procesos y productos (Fenton, 1997) [21]. No existe una implementación perfecta como no existe una planificación perfecta. Nuestras iniciativas pueden tener fallos conceptuales, no estar logrando los objetivos para que las habíamos planteado. Es mediante las mismas métricas que podemos retroalimentar el proceso de planificación para entender como los detalles de implementación contrastan con la estrategia.

Como vemos de las métricas establecidas en las iniciativas propuestas, hay una que vale para todas: el tiempo de completamiento estimado versus el tiempo invertido actualmente. Esta métrica es muy importante porque además de medir el avance de la iniciativa nos permite entender si nuestros procesos son eficientes como habíamos estimado o menos. A través de esta métrica podemos entender si necesitamos cambiar o mejorar los procesos de implementación de las iniciativas.

Enfocando nuestro proceso de investigación en la cultura de ciberseguridad tratamos de medir también la satisfacción de los empleados en participar en los cursos de capacitación. Mediante estos cursos, no solamente queremos elevar el nivel de conocimientos de nuestros trabajadores, sino mejorar sus comportamientos hacia la seguridad de la información.

7. Siguientes Pasos

Una vez desarrollada la estrategia de seguridad de la información tendremos que medirla y mejorarla continuamente. El mundo de la tecnología avanza rápido, y los riesgos y las amenazas que conlleva para las organizaciones también. Cada día hay nuevas vulnerabilidades, nuevas técnicas de ataque, nuevas lecciones para aprender.
Los marcos normativos siguen evolucionando con la tecnología y los requerimientos legales. Así tendrá que evolucionar también nuestra estrategia de seguridad [21]. Para esto hemos planteado las métricas de nuestras iniciativas que nos ayudaran en este proceso futuro. La ciberseguridad es un habilitador para el desarrollo del potencial de la digitalización de las organizaciones y la estrategia de seguridad representa la guía para manejarlas [22].

El proceso de mejora continua más importante según la metodología que hemos decidido de adoptar será la medición futura de la cultura de seguridad. Midiendo nuevamente la cultura de seguridad de la información usando los siete indicadores propuestos podremos averiguar si hemos logrado una transformación cultural dentro de nuestra organización. Aquí podremos encontrar nuevos patrones, hallazgos y desafortunadamente también problemas que requerirán aplicar nuestra metodología otra vez, para investigar, analizar, planificar controles e implementarlos. Nuevamente habrá que examinar nuestro entorno, conocer cómo se mueven los demás. Sobre todo, los más grandes. Con pequeños pasos nos acercaremos a los estándares estudiados, aumentando nuestro nivel de madurez.
Acabamos de poner las fundamentas para crecer estratégicamente, mejorar y optimizar nuestras iniciativas para que se adapten a los escenarios futuros.

8. Guía de ciberseguridad para PYME

En resumen, lo que hemos presentado como caso de estudio nos ha permitido construir una metodología que podemos reutilizar para guiarnos en enfrentar la ciberseguridad en una organización.

Antes de todo, tendremos que examinar nuestra organización. No todas las organizaciones son iguales, tenemos una visión y misión específica que nos caracteriza. Tratamos de interiorizar estos aspectos para entender mejor que necesita nuestra organización de cara a la ciberseguridad.

Una vez examinado los principales procesos de nuestra organización, tenemos que analizar la información recolectada para sacar los hallazgos que nos permiten medir nuestra situación actual. Analizando los hábitos de nuestros trabajadores relacionados con nuestros objetivos podemos medir la cultura de ciberseguridad. El aspecto cultural es fundamental, porque permite medir los efectos que las iniciativas de seguridad tienen sobre nuestros trabajadores.

Individuados los problemas, hay que pensar cómo solucionarlos. La metodología que proponemos se basa en 4 objetivos principales que construyen la estrategia de seguridad de la información:

Organización Estructural: importante porque una estructura ordinada permite encontrar rápidamente los problemas y esto significa solucionarlos antes.

Cultura de Trabajo: importante porque representa una actitud espontanea que mira a no generar problemas en primera instancia.

Concienciación de Seguridad: importante porque el mundo de la tecnología es en continua evolución, y es necesario conocer las técnicas de *los malos* para poderse defender.

Gobierno de la Seguridad: importante porque permite orquestar todos aquellos procesos que componen la estrategia de seguridad: las iniciativas, los controles, los servicios de seguridad implementados, etc.

Una vez que se han planificado los controles para lograr los objetivos, hay que proponer e implementar iniciativas concretas que puedan cumplir dichos objetivos. La metodología suele basar estas iniciativas en 5 funciones principales que propone el Cybersecurity Framework del NIST: Identify, Detect, Protect, Respond, Recover. Estas funciones proporcionan soluciones para los escenarios actuales de riesgos y amenazas de la ciberseguridad.

Finalmente hay que cuestionar nuestra estrategia, medirla y eventualmente mejorarla.

9. Bibliografía

[1] *NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. (2018). Gaithersburg, MD. Retrieved from http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[2] Mcgraw, G., Migues, S., & West, J. (n.d.). *BSIMM9*. Retrieved from https://www.bsimm.com/content/dam/bsimm/reports/bsimm9.pdf

[3] Software Security Terms & Glossary | BSIMM. (n.d.). Retrieved January 17, 2019, from https://www.bsimm.com/about/glossary.html

[4] Langner, R., & Pederson, P. (2013). *Bound to Fail: Why Cyber Security Risk Cannot Simply Be Managed Away*. Retrieved from http://www.inl.gov/scada/publications/d/inl_nstb_common

[5] Políticas de seguridad para la pyme | INCIBE. (n.d.). Retrieved January 17, 2019, from https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[7] CLTRe Insight – CLTRe – the Yardstick of Culture. (n.d.). Retrieved January 17, 2019, from https://get.clt.re/insight/

[8] Ajzen, I. (2011). Psychology & Health The theory of planned behaviour: Reactions and reflections Icek Ajzen The theory of planned behaviour: Reactions and reflections. *Psychology and Health*, *26*(9), 1113–1127. http://doi.org/10.1080/08870446.2011.613995

[9] NIST Special publication 800-53 Rev 5 | NIST 2018

[10] ISO/IEC 27001:2013(en), Information technology — Security techniques — Information security management systems — Requirements. (n.d.). Retrieved January 17, 2019, from https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

[11] Software Security Framework | BSIMM. (n.d.). Retrieved January 17, 2019, from https://www.bsimm.com/framework.html

[12] *Transforming cybersecurity : using Cobit 5.* (2013). ISACA. Retrieved from https://books.google.com.pe/books/about/Transforming_Cybersecurity_Using_COBIT_5.html?id=_AhkAgAAQBAJ&printsec=frontcover&source=kp_read_button&redir_esc=y#v=onepage&q&f=false

[13] ISO/IEC 27032:2012 - Information technology -- Security techniques -- Guidelines for cybersecurity. (n.d.). Retrieved January 17, 2019, from https://www.iso.org/standard/44375.html

[14] SANS CIS Top 20 Controls. (n.d.). Retrieved January 17, 2019, from https://www.cisecurity.org/controls/

[15] ISO/IEC 27031:2011 - Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity. (n.d.). Retrieved January 17, 2019, from https://www.iso.org/standard/44374.html

[16] Bowen, P., Hash, J., Wilson, M., Gutierrez, C. M., Cresanti, R., & Jeffrey, W. (2006). NIST 800-100 *Information Security Handbook: A Guide for Managers Technology Administration*. Retrieved from https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50901

[17] Roer, K., & Petric, G. (2017). *Indepth Insights Into the Human Factor: The Security Culture Report 2017*. CreateSpace Independent Publishing Platform. Retrieved from https://books.google.com.pe/books?id=wZImtAEACAAJ

[18] Cloud Analytics Mobile Social Security | IBM UK Apprentice Blog. (n.d.). Retrieved January 17, 2019, from https://ibmapprentice.wordpress.com/tag/cloud-analytics-mobile-social-security/

[19] Roer, K. (n.d.). *Build a security culture*. Retrieved from https://books.google.com.pe/books/about/Build_a_Security_Culture.html?id=d4k3DwAAQBAJ&printsec=frontcover&source=kp_read_button&redir_esc=y#v=onepage&q&f=false

[20] Svensson, L., Snis, U., Sørensen, C., Fgerlind, H., Lindroth, T., Magnusson, M., … Kautz, K. (2000). The Challenge of Metrics Implementation.

[21] *IBM X-Force Threat Intelligence Index 2018 Notable security events of 2017, and a look ahead*. (2018). Retrieved from https://microstrat.com/sites/default/files/security-ibm-security-solutions-wg-research-report-77014377usen-20180329.pdf

[22] IBM Security Summit 2017 - La ciberseguridad como habilitador de la transformación digital - YouTube. (n.d.). Retrieved January 17, 2019, from https://www.youtube.com/watch?v=LfUWi9b8_Lk