“Universidad Internacional de La Rioja en México”

Ciberdelitos y Regulación de la Ciberseguridad

Proyecto:

Caso grupal: Confección de una evaluación de impacto en protección de datos (EIPD)

Profesor:

OSCAR MANUEL LIRA

Autor:

Juan Luis Cruz Aristeo.

Fecha de entrega:

17/06/2024

INDICE

Introducción

En la actualidad muchas organizaciones se han visto afectadas por ataques cibernéticos, los cuales las han llevado a tener a algunas organizaciones perdidas mínimas, mientras que para a otras a pérdidas totales, debido a filtraciones, manipulación y destrucción de sus activos más valiosos. Sin duda es una realidad que actualmente tecnología a avanzado a gran velocidad, a la par también nacieron nuevas formas de perjudicar a aquellos que son más vulnerables, mediante diferentes formas que hacen uso poco ético de estas nuevas tecnologías.

Debido a esta realidad mucho gobiernos, organizaciones, academias y profesionales, desarrollaron marcos de seguridad para poder anticiparse y defenderse de estas amenazas. Estos marcos nos brindan guías, procesos y formas de asegurar los activos más valiosos de las organizaciones públicas y privadas. Un ejemplo es el marco de seguridad CSF (Cybersecurity Framework), que no solo ayuda a identificar y gestionar los riesgos de la ciberseguridad, también fomenta la cultura de la seguridad dentro de las organizaciones, mediante la capacitación constante a los miembros de la organización, su enfoque es estructurado y se puede adaptar a cualquier tipo de organización, esto facilita a que dentro de las organizaciones se pueda tener una buena comunicación entre las diferentes partes interesadas comprendiendo adecuadamente que es lo que se quiere lograr, lo que permite que todos puedan trabajar hacia el objetivo en común que es la seguridad de los activos valiosos de la organización.

En este esta actividad objetivo es realizar un análisis detallado del marco de ciberseguridad CSF (Cybersecurity Framework) con la finalidad de desarrollar los 3 primeros pasos en el proceso de identificación los cuales se describen en el documento que compartió el docente a cargo de la materia.

Descripción de la organización.

La organización OLIX S.A.

OLIX S.A. es una empresa mexicana fundada en 2014, dedicada a brindar servicios tecnológicos. Actualmente, OLIX S.A. está en pleno crecimiento y cuenta con 115 empleados. Su sede se encuentra en Ciudad de México.

Su misión es: Innovar y proporcionar servicios IT para empresas de diferentes sectores, mejorando su eficiencia e integrándolas al mundo digital. Mediante el desarrollo de páginas web diseñadas para destacar a las empresas en su sector la cuales siempre estarán disponibles y seguras.

Su visión es: Ser líder en el mercado de servicios IT a nivel nacional a través de la innovación constante, la calidad y el servicio al cliente.

Servicios Ofrecidos

OLIX S.A. ofrece desarrollo web personalizado, incluyendo diseño, creación y mantenimiento de sitios web. Este servicio está orientado a la disponibilidad y seguridad además de cumplir con las especificaciones del cliente. Diseñando sitios web para organizaciones de distintos sectores en diferentes partes de México, utilizando diversas tecnologías de desarrollo web, con el objetivo de que las páginas sean innovadoras y atractivas para los usuarios. Además, realizamos mantenimiento constante para mantener los sitios actualizados.

Actividades Incluidas:

- Análisis de requisitos.
- Selección de tecnologías y herramientas.
- Desarrollo Front-End. - Desarrollo Back-End.
- Pruebas.
- Despliegue y mantenimiento.

El marco de seguridad CSF (Cybersecurity Framework)

¿Qué es el Cybersecurity Framework?

El Cybersecurity framework, es un marco de seguridad que fue solicitado, por parte del presidente de los estados unidos de américa en el año 2013. Este marco de seguridad fue desarrollado por el NIST (Instituto Nacional de Estándares y Tecnologías). Su objetivo era proteger los 13 sectores infraestructuras críticas, que fueron identificadas por los estados unidos.

Este marco se creó para identificar normas y directrices de seguridad, toman parte de algunas que ya existían, el objetivo era que fueran aplicables en todos los sectores, para así tener un marco flexible y adaptable, facilitando la gestión de riesgos y la implementación de tecnologías en cualquier tipo de organización.

Algunos de los estándares que se tomaron como base fueron los:

- NIST SP 800-53 Rev.4
- ISO/IEC 27001:2013
- COBIT 5
- CIS CSC

Además de la participación de las diferentes partes interesadas como el gobierno, industria y la academia.

¿Cómo trabaja el CSF?

El CSF está conformado por 3 componentes.

1. Freamwork Core (núcleo del marco)
2. Niveles de implementación
3. Perfiles.

Freamwork Core (núcleo del marco)

El primer componente Freamwork Core (núcleo del marco) básicamente es la parte central del marco, ya que este consiste en las actividades y objetivos que se desean alcanzar. El core consta de 3 partes: Funciones, Categorías y Subcategorías.

- Su estructura se compone por 5 funciones.
    1. Identificar
    2. Proteger
    3. Detectar
    4. Responder
    5. Recuperar

- Se compone por 23 categorías, estas abordan temas técnicos, de personas y de procesos, proporcionando una visión más detallada de los objetivos de la ciberseguridad.

- Se compone por 108 subcategorías. Este nivel es mucho más específico, pues son declaraciones de resultados que ofrecen consideraciones específicas para crear o mejorar un programa de ciberseguridad.

Niveles de implementación

Los niveles de implementación, describen el grado que una organización adopta para sus prácticas de gestión de riesgos, estos niveles no reflejan si una organización está fuertemente protegida o no, como si describiera la madures de sus prácticas, es más parecido a establecer un nivel deseado por la organización, únicamente que cumpla los objetivos de reducir el riesgo de ciberseguridad a niveles aceptables.

Niveles:

Nivel 1 Parcial: en este nivel, las prácticas de gestión de riesgos de ciberseguridad no están formalizadas.

Nivel 2 Riesgo Informado: En este nivel, las prácticas de gestión están establecidas, pero tienen procedimientos informales y muchos de ellos no están documentados.

Nivel 3 Repetible: En este nivel una organización tiene políticas y procedimientos de ciberseguridad documentados. Realiza evaluaciones y sigue mejorando sus prácticas basadas en estas evaluaciones.

Nivel 4 Adaptativo: En este nivel un ejemplo es una organización gubernamental de alta seguridad, la cual hace uso de herramientas avanzadas de análisis y tiene un equipo dedicado a la ciberseguridad.

Perfiles

Básicamente un perfil es la representación de la organización con respecto su situación en términos de ciberseguridad, compara la que tiene con lo que quiere, mediante una evaluación completa analizando sus prácticas, para posteriormente basarse en los resultados para establecer los requisitos y objetivos que se desean.

Para este proceso se diseñan 2 perfiles

Perfil actual: Evaluación completa dele estado actual de las prácticas de ciberseguridad en la organización.

Perfil objetivo: Se basa en las evaluaciones, los requisitos y los objetivos que se desean alcanzar.

Finalmente se comparan y se identifican las brechas para establecer un plan de acción.

¿Cómo usar el CSF?

EL Cybersecurity framework (CSF) es una herramienta flexible, es decir se adapta a cualquier organización con el objetivo de gestionar sus riesgos. No importa su tamaño o sector. Este marco en lugar de introducir nuevos controles, hace uso de los controles ya establecidos.

Algunas de las estrategias para adaptar el marco CSF, son las siguientes:

Revisión básica de prácticas de ciberseguridad: Esta estrategia consiste en que una organización puede hacer uso del CSF como parte de su proceso, identificando brechas en el enfoque actual y desarrollar un plan para mejorar.

Creación o mejora de un programa de ciberseguridad: El CSF puede servir de base para crear todo un programa o mejorarlo, esta estrategia consta de siete pasos para guiar este proceso, recordando que la ciberseguridad se debe tomar como proceso continuo, es decir siempre debe estarse mejorando y evaluando continuamente.

Pasos para la creación o mejora de un programa de ciberseguridad:

Paso 1: Priorizar y determinar el alcance.

Paso 2: Orientación.

Paso 3: Crear un perfil.

Paso 4: Realizar una evaluación de riesgos.

Paso 5: Crear un perfil objetivo.

Paso 6: Determinar, analizar y priorizar las brechas.

Paso 7: Implementar el plan de acción.

Este trabajo solo abarcara los primeros 3 pasos para el uso de este marco por lo que se desarrollara una descripción para comprenderlos más a profundidad y entender cómo se realizan.

Paso 1: Priorizar y determinar el alcance (ANALISIS).

En este paso debemos identificar los objetivos y prioridades de alto nivel de la organización. De esta forma podemos determinar el alcance, la línea de negocio o procesos que serán abordados. Esto significa que hay que definir qué áreas, sistemas, procesos específicos se incluirán en el programa de ciberseguridad.

Identificación de los objetivos del negocio y las prioridades de alto nivel

Algunos ejemplos:

Protección de datos: se asegura la información sensible.

Continuidad del servicio: garantizas que los servicios estén disponibles.

Cumplimiento normativo: Cumplir con leyes y regulaciones aplicables.

Determinar el alcance, la línea de negocio o procesos que serán abordados.

Básicamente es incluir las actividades, sistemas y procesos.

Ejemplo Almacenamiento de datos de clientes: aquí deberíamos incluir todos los sistemas y procesos que gestionan.

Paso 2: Orientación (ANALISIS).

Este paso consiste en identificar los sistemas y activos vinculados, es decir hay que reconocer y catalogar todos los componentes tecnológicos. También hay que identificar requisitos legales o regulatorios, lo que implica determinar las leyes, normas y regulaciones que se deben cumplir para evitar sanciones legales.

Ejemplos de componentes tecnológicos:

Sistemas y activos vinculados al alcance: servidores de bases de datos, sistemas de pago en línea, aplicaciones web, etc.

Ejemplos de leyes y normas.

GDPR (General Data Protection regulation): Es una regulación de la unión europea, la cual indica que se debe obtener el consentimiento explícito de los usuarios antes de recopilar sus datos y permitirles accedes y eliminar su información cuando de lo deseen. Lo que significa que la empresa debe cumplir con ello, garantizando el cumplimiento de leyes y normas.

Paso 3: Crear un perfil (ANALISIS).

El objetivo de este paso es realiza una evaluación del estado actual de las organizaciones con respecto a su programa de ciberseguridad, analizando 3 áreas clave: personas, procesos y tecnología. De esta forma se pueden identificas los puntos fuertes y las parte vulnerables que se tienen en ese momento, así obtenemos como resultado una base sólida para planificar mejoras.

¿En qué consiste la evaluación?

La evaluación consiste en examinar la estructura de la organización en las 3 áreas clave mencionadas, aquí se detallarán algunos ejemplos.

Personas: El personal con el que cuenta el equipo TI de la organización, ¿Cuántos de ellos tiene formación específica en ciberseguridad?

Procesos: Revisar si hay procedimientos de seguridad existentes, documentación, y como gestionan los procesos críticos, como la respuesta a incidentes, si son gestionados manualmente o son automatizados.

Tecnología: Analizar la infraestructura tecnológica, como los sistemas y sus actualizaciones, sus configuraciones de seguridad y las herramientas de monitorización.

Desarrollo de los 3 primeros pasos de CSF en la organización OLIX S.A.

Paso 1 Priorizar y determinar el alcance de los objetivos en OLIX S.A.

Determinando los objetivos de negocio para OLIX S.A.

En base a la misión de OLIX S.A se destaca que el servicio que brinda a sus clientes es el desarrollo web que está orientado a la disponibilidad y seguridad. Debido a esto los objetivos del negocio de OLIX S.A. estarán dirigidos a los objetivos de su misión ya que su meta principal es tener la confianza de sus clientes la cual lograra, cumpliendo la misión de la empresa.

Objetivos de negocio de OLIX S.A.

Protección de datos: este objetivo se centra en garantizar la seguridad y confidencialidad de la información personal de los clientes mediante la implementación de cifrados y controles de accesos.

Gestión de incidentes de seguridad: Este objetivo se centre en crear un programa de respuestas a incidentes de ciberseguridad para detectar, responder y recuperarse rápidamente ante cualquier incidente.

Desarrollo del talento humano: Este objetivo se centra en invertir en la formación y desarrollo profesional de los empleados para mantener un equipo capacitado y consiente sobre las amenazas cibernéticas, teniendo una cultura de seguridad dentro de la organización.

Seguridad de infraestructura: Este objetivo se centra en la protección de la infraestructura tecnológica, que incluye servidores, redes y dispositivos.

Continuidad del servicio: Este objetivo se centra en implementar planes de recuperación ante desastres y su continuidad, de esta forma los servicios estarán siempre disponibles, minimizando tiempo de inactividad.

Determinando el alcance del programa de ciberseguridad dentro de OLIX S.A.

En este apartado vamos a definir las áreas, sistemas, procesos y datos específicos, que ayudaran a focalizar los esfuerzos y recursos hacia el cumplimiento de los objetivos del negocio. Por lo que para poder delimitar adecuadamente el alcance a continuación el desarrollo.

Protección de datos

- Departamento de TI: Este departamento se encargará de implementar y mantener las medidas de seguridad en sistemas y bases de datos
- Equipo de desarrollo de web: el equipo de desarrollo web, tendrá que implementar prácticas de codificación seguras para poder proteger los datos que tendrán las páginas.

Gestión de incidentes de seguridad:

- Equipo de respuesta a incidentes: Este equipo estará a encargado de detectar, responder y gestionar incidentes de seguridad.
- Departamento de TI: El departamento de TI apoyara brindara soporte técnico y herramientas para la gestión de incidentes,

Desarrollo del Talento Humano:

- Departamento de recursos Humanos: Se encargada de gestionar programas de formación y desarrollo profesional en ciberseguridad, para concientizar a la organización.
- Departamento de TI: Apoyara brindando contenido técnico, asegurando la formación adecuada en tema de ciberseguridad.

Seguridad de infraestructura:

- Departamento de TI: gestionara que el equipo de redes implemente y mantenga la seguridad de las redes y sistemas de comunicación, además de asegurar la protección de los equipos y las instalaciones.

Continuidad del servicio:

Equipo de gestión de riesgos: Este equipo está encargado de identificar y desarrollar programas de mitigación de riesgos que puedan afectar la disponibilidad de las páginas web.

Departamento de TI: se encargará de gestionar sistemas de respaldo y recuperación de datos.

Paso 2 Orientación.

Este paso consiste en cumplir las siguientes 2 condiciones:

1. Identificar los sistemas y activos vinculados al alcance: Se realiza una lista de todos los componentes tecnológicos de la organización que se relacionan con la ciberseguridad. Estos componentes pueden ser tanto equipos físicos como programas y aplicaciones. La importancia de realizar esto es para enfocarnos en proteger los más vulnerables.
2. Identificar los requisitos legales y regulatorios: hay que conocer y entender las leyes, normas y regulaciones que la empresa debe cumplir para evitar problemas legales, sanciones y multas. Las cuales están diseñadas para proteger la privacidad y seguridad de los datos. Lo que ayuda a evitar multas y sanciones legales, además de que ayuda a mejorar la confianza y reputación de la organización.

Identificación de los sistemas y activos vinculados al alcance.

Servidores de la organización

- servidores físicos y virtuales donde se almacenan los datos más importantes de la organización OLIX S.A.

Plataformas de control de versiones:

- son las herramientas utilizadas para gestionar y clasificar en versiones los códigos fuentes de las páginas web.

Sistemas de pago en línea:

La plataforma que permiten y procesan pagos.

Computadoras y dispositivos móviles:

- todos los equipos utilizados para el desarrollo web.

Redes y dispositivos de red:

- todos los equipos que se conectan y protegen la red interna de la organización.

Sistemas de respaldo y recuperación

- Herramientas y procesos que tendrán copias de seguridad y que ayudarán a recuperar datos en caso de fallos.

Requisitos legales o regulatorios

- **Ley federal de protección de datos personales en posesión de los particulares (LFPDPPP):** Esta ley establece que se deben manejar los datos personales de manera responsable y transparente en México.
- **Norma Oficial Mexicana NOM-151-SCFI-2016:** Es una norma que establece los requisitos para la conservación de mensajes de datos y documentos electrónicos, que incluyen su autenticidad, integridad y fiabilidad.
- **GDPR (General Data Protection Regulation):** Es un reglamento establece lo siguiente.
    - Obtener consentimiento explícito de los usuarios antes de recopilas sus datos.
    - Permitir a los usuarios acceder, saber en qué son utilizados sus datos y eliminar su información personal en el momento que deseen.

- **PCI DSS (Payment Card Industry Data Security Standard):** Son un conjunto de normas de seguridad para manejar datos de tarjetas de crédito.
- **ISO/IEC 27001:** Es una norma internacional para la gestión de seguridad de la información.

Enfoque de riesgo general activos

Este enfoque se refiere a la identificación y evaluación de los riesgos asociados a los sistemas y activos tecnológicos de la organización. Ayuda a entender que amenazas y vulnerabilidades que pueden afectar a OLIX S.A. y poder gestionarlas para brindar una mejor protección de los activos críticos.

Amenazas externas:

- **Ciberataques**: esta amenaza se centra en intentos de acceso no autorizado a los sistemas de OLIX S.A. por medio de posibles ataques DDOS.
- **Malware**: Existe la amenaza de adquirir un software malicioso por diferentes medios, como unidades USV, descarga de programas de usuarios desconocidos. Lo que podría terminar en encriptación de datos críticos.
- **Phishing**: Una amenaza que se centra en intentos de obtener información sensible, engañando a personas de la organización, haciéndose pasar por una entidad de confianza, adquiriendo credenciales y acceso a información crítica.
- **Ataques de Man- in-the-Middle(MitM**): Intercepción de comunicaciones entre usuarios y servidores, por medio de puntos de acceso vulnerables, lo que permite capturar datos sensibles.

Amenazas internas:

- **Errores Humanos**: esta amenaza se centra en acciones no intencionadas que pueden comprometer la seguridad de la organización, como vulnerabilidades en la programación de las páginas web, envió de información a destinatarios incorrectos.
- **Mal uso de privilegios**: Algún empleado o desarrollador accede a datos importantes de la empresa fuera de su área de trabajo.
- **Fallos de hardware o software**: Problemas técnicos que afecten la seguridad de la organización, como fallos en discos duros.
- **Acceso No autorizado**: Esta amenaza va de la mano de empleados descontentos que podrían sabotear los sistemas, compartiendo las credenciales a terceros.

Vulnerabilidades:

- Sistemas sin parches: Esta es una de las vulnerabilidades que se encuentran con mayor frecuencia dentro de las organizaciones, se trata de softwares que no han sido actualizados con las ultimas correcciones de seguridad, podrían permitir filtraciones debido a esta falta de actualizaciones.
- Configuraciones de seguridad deficientes: Esta vulnerabilidad consiste en que muchas veces las organizaciones tienen a no tener buenas prácticas de seguridad, por ejemplo, servidores con puertos abiertos innecesarios.
- Falta de capacitación en ciberseguridad: Esta vulnerabilidad se centra en la falta de capacitación al personal, en el ámbito de la ciberseguridad, ejemplo, desarrolladores que no conocen las implicaciones de la inyección de código.
- Autenticación y autorización inadecuadas: Esta vulnerabilidad se refiere a los métodos de acceso que no son seguros, por ejemplo, el uso de contraseñas predeterminadas o débiles.

Paso 3: Crear un perfil actual.

En este paso, se busca realizar una evaluación del programa de ciberseguridad actual de OLIX S.A. la evaluación se enfoca en tres áreas clave, las personas, procesos y tecnología. Esto con el objetivo de identificar las fortalezas y debilidades del programa. Así la empresa podrá obtener una visión clara de su estado actual en lo que respecto a la ciberseguridad. De esta forma podrá planificar las mejoras de forma más eficiente, asegurando una buena protección.

Áreas de evaluación:

Personas:

Personal de OLIX S.A.: OLIX S.A. es una organización que ofrece servicios de desarrollo web, por lo que su personal esta principalmente enfocado al desarrollo y mantenimiento de las páginas de los clientes.

- Desarrollo software (45 personas): Este personal está enfocado realizar las actividades de Desarrollo front-end, Desarrollo Back-end y Desarrollo full-stack. Además, cuenta con algunos especialistas en UX/UI.
- Operaciones IT (30 personas): Las actividades de este personal son la administración de sistemas, administración de redes y especialistas en soporte técnico.

- **Ciberseguridad** (5 personas): Esta es el área más pequeña de la empresa, únicamente se dedica a monitorear incidentes, revisión de código capacitar el área de desarrollo y el área de operaciones TI sobre temas de ciberseguridad, por último, se encarga de implementar soluciones de seguridad.
- Recursos Humanos (15 personas): Las actividades de este personal se centra en la gestión del talento y documentación general de la organización. (**No cuenta con capacitación sobre temas en ciberseguridad)**
- Finanzas y administración (15 personas): El personal se centra en las actividades como supervisión de la contabilidad general de la empresa, estados financieros, analizar costos de producción, preparar y presentar declaraciones de impuestos. (**No cuenta con capacitación sobre temas en ciberseguridad**)
- Alta dirección (5 personas): son los responsables de la toma de decisiones estratégicas y la dirección general de la empresa.

Procesos:

- **Estrategia:** La estrategia de ciberseguridad de OLIX no está alineada sus objetivos del negocio, que incluyen la protección de datos de clientes y la continuidad del servicio. Actualmente se centra únicamente en un método reactivo, respondiendo y monitoreando lo que sucede a cada momento. Esta estrategia se empezó a seguir cuando OLIX empezó a desarrollar proyectos más amplios. Actualmente debido a la gran demanda que ha tenido y que los clientes que empiezan a surgir tienen requisitos más estrictos, OLIX tiene planes (de alinear su estrategia de ciberseguridad con los objetivos del negocio).
- **Políticas y Procedimientos:** OLIX es una organización que no cuenta con políticas claras sobre los dispositivos dentro de la organización, únicamente monitorea los dispositivos registrados en la empresa, los cuales cuentan con un software de seguridad aprobado por el equipo de ciberseguridad, estos equipo son con los que trabajan lo diferentes equipos y solo los departamentos de desarrollo y operaciones TI, tienen procedimientos más detallados para la seguridad de sus activos, los demás departamentos dependen completamente del equipo de ciberseguridad.
- **Gestión de incidentes y recuperación ante desastres:** En OLIX el equipo de ciberseguridad tiene procedimientos para la gestión de incidentes y ha establecido algunos protocolos de recuperación ante desastres, capacitando al equipo de desarrollo y operaciones TI.

Tecnología:

- **Capacidades y configuraciones:** OLIX emplea algunas herramientas para poder monitorizar la seguridad en la infraestructura tecnológica, le permite identificar incidentes y responder ante ellos. Por otro lado, OLIX utiliza cifrado avanzado como HTTPS, además de cifrar los discos duros de la organización, con el objetivo de asegurar la confiabilidad. Sin embargo, debido a que el equipo de ciberseguridad no cuenta con tanto personal y se ve saturado por las actividades que debe realizar en la empresa no lleva acabo muy a menudo las auditorias de seguridad, las cuales son necesarias para mejorar las configuraciones.
- **Vulnerabilidades: En** OLIX quienes realizan evaluaciones de vulnerabilidades en las páginas web, son los mismos desarrolladores y el equipo de operaciones TI, posteriormente si se encuentran vulnerabilidades se actualizan las páginas con parches. Aun que muchas veces OLIX recibe mensajes de los clientes, en los cuales les indican que alguien detecto una falla en las páginas.
- **Operaciones y Contratos:** Las operaciones del equipo de ciberseguridad están documentas, pero no se siguen estrictamente, debido a esto no está garantizada la consistencia y en la respuesta a incidentes se tiene poca eficacia. Por otro lado, no mantiene contratos de soporte con proveedores externos, depende completamente de sus propios medios.

Conclusión:

Actualmente muchas organizaciones están reforzando el área de la ciberseguridad, esto es debido a muchos factores, principalmente a la migración virtual ya que esto hace que las empresas gasten menos en equipos físicos, pero conlleva a que mejoren sus prácticas de seguridad y si bien muchas de estas organizaciones ya contaban con algunas prácticas otras apenas empiezan a crear sus bases. El marco CSF, sin duda es una buena guía para crear un sistema adecuado a las diferentes organizaciones, nos damos cuenta que analiza los objetivos de la organización, identifica que activos que se involucran, para poder acoplarse a la organización. Esto lo hace por medio de los diferentes pasos que tienen como objetivo analizar a fondo la organización en la que se quiere implementar el marco, lo que lo hace interesante es la forma en la que se desarrolla cada paso, me pareció muy interesante entender que este marco se desarrolló no para remplazar, los sistemas ya existentes, más

bien el hecho de tomar un poco de todo con el objetivo de poder establecer un marco que cualquier organización pueda utilizar, que sea flexible y que se acople a las diferentes áreas.

Durante este trabajo me di cuenta que en México muchas empresas pequeñas no siguen un marco de seguridad para la protección de datos críticos, esto lo digo basado en mi experiencia, en las empresas que he trabajado, no cuentan ni siquiera con equipo para respuesta a incidentes, no hay capacitaciones con respecto a la ciberseguridad, incluso no hay protocolos de recuperación. Debido a esto no contaba con un ejemplo para desarrollar este proyecto, por lo que decidí tomarme la libertad de diseñar OLIX, en donde tuve muchas complicaciones para poder moldear la organización a favor de que se entienda como desarrollar el marco en esta organización, sin duda creo que ahora comprendo mucho mejor la identificación de los sistemas y activos, la priorización y determinación del alcance lo que se me hace muy importante para poder determinar en que si hay que implementar procesos, políticas y configuración para protegerlo adecuadamente.

Hoja de asistencias.

Hoja de control de actividad grupal **<Nombre y apellidos del primer miembro del equipo >**			
	Marcar con una **X** lo que proceda		
Asistencia a reuniones de equipo	Asistencia a una sesión o ninguna	Asistencia a dos sesiones	Asistencia a tres sesiones
- Juan Luis Cruz Aristeo			X
-Erick Ramirez Ascencio	X		
- Integrante 3	X		
- Integrante 4	X		
- Integrante 5	X		
Tareas o entregas a realizadas	Ninguna o una tarea	Dos tareas	Tres tareas
- Integrante 1			X
- Integrante 2	X		
- Integrante 3	X		
- Integrante 4	X		
- Integrante 5	X		