Máster Universitario en Ciberseguridad y Privacidad (MUCIP)

ANEXO 5
PROPUESTAS DE PROYECTOS

Universitat Oberta de Catalunya

Natividad García Lacárcel

INDICE

PROYECTOS 2
PLAN DE EJECUCIÓN 15
PRESUPUESTO 18

PROYECTOS

Proyecto 1: Definir políticas de seguridad de la información
Responsable de proyecto: Departamento de sistemas y Dirección
Prioridad: Alta
Activos afectados: Datos
Objetivo:

- Crear el documento formal de las políticas de seguridad de la empresa estableciendo controles y métodos de divulgación. Definir las políticas de seguridad de acuerdo, al análisis de la norma ISO 27001.
- Establecer controles de seguridad con el fin de velar el cumplimiento de las políticas de seguridad establecidas.
- Fijar la metodología y estrategia de divulgación de las políticas de seguridad para que todas las personas que tengan acceso a la información la conozcan.
- Elaborar un plan de monitoreo para la revisión periódica de las políticas de seguridad de la información.

Descripción:
El documento de política de seguridad expresa la intención e instrucción global de la seguridad que formalmente ha sido expresada por la Dirección de la organización. Pretende definir las necesidades conforme a la norma ISO 27001:2013 enfocados en los procesos de la organización en cuanto a políticas de seguridad de la información.
Creando nuevas políticas necesarias que permitan fortalecer el sistema de información. Modificando políticas existentes de manera que sean claras y abarquen el contenido necesario que permita a la organización crear un sistema de gestión de la información conforme a estándares y leyes.

Motivación:
Corregir problemas y mejorar los resultados del análisis de riesgos. Mejora del anexo 5 - 27001

Controles:
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.
18.2.1 Revisión independiente de la seguridad de la información
18.2.2 Cumplimiento de políticas y estándares de seguridad

Medición:

- Grado de despliegue y adopción de las políticas en la organización (medido por auditoría, gerencia o auto-evaluación).
- Revisión anual del cumplimiento de las políticas de seguridad.

Tiempo: 2 meses

Coste: 1000€

Proyecto 2: Mejora del CPD
Responsable de proyecto: Departamento de sistemas
Prioridad: Alta
Activos afectados: Instalaciones – CPD, Hardware - Servidores y equipos
Objetivo:

- Mejora de la climatización para garantizar la disponibilidad de los sistemas informáticos allí presentes.
- Mejora del sistema eléctrico del CPD para evitar la pérdida de disponibilidad como consecuencia de carencia del fluido.
- Mejora del apagado ordenado de los servidores en situaciones de fallo de la climatización o del fluido eléctrico.
- Revisión seguridad acceso al CPD y perímetro de seguridad

Descripción:
Los servidores ubicados en el CPD son claves para el negocio de la organización. Se requiere una disponibilidad continua de los servicios de información configurados en el mismo. Por esta causa se hace necesario la revisión del sistema de climatización, así como del sistema eléctrico.
Para ello se precisará un estudio de las necesidades del CPD, cálculo de la potencia eléctrica requerida por los servidores y cálculo de la capacidad de refrigeración para mantener el espacio a una temperatura óptima.
Mejora de la red eléctrica habilitando las instalaciones para el número de servidores habidos y planificando posibles ampliaciones.
Comprobación de la eficiencia del sistema de alimentación ininterrumpida y en caso de no cumplir los requerimientos valorar su posible sustitución.
Generar la documentación sobre el procedimiento a seguir ante incidentes.

Motivación:
Corregir problemas y mejorar los resultados del análisis de riesgos. Mejora del anexo 11 - 27001

Controles:
11.1.1 Perímetro de seguridad física
11.1.2 Controles de entrada físicas
11.1.4 Protección contra amenazas externas y del ambiente
11.2.1 Emplazamiento y protección del equipo
11.2.2 Instalación de suministro
11.2.3 Seguridad del cableado
11.2.4 Mantenimiento del equipamiento

Medición:

- Pruebas anuales de simulacro de caída de suministro eléctrico.
- Pruebas anuales de simulacro de fallo en el sistema de climatización.
- Documentación ante estos incidentes para mejorar.
- Control del número de incidentes anuales que se producen al año.

Tiempo: 4 meses
Coste: 2500€ Instalación y puesta en marcha sistema de climatización.
1500€ Incremento potencia contratada. Mejora de la instalación eléctrica aumentando el número de puntos.

Proyecto 3 – Control de acceso
Responsable de proyecto: Departamento de sistemas y Dirección
Prioridad: Alta
Activos afectados: Datos, Hardware, Red, Personal
Objetivo:

- Establecer, actualizar y documentar los procesos que intervienen en las actividades de seguridad física y control de acceso a los sistemas de información.
- Actualizar los procedimientos sobre el tratamiento de seguridad de la información para usuarios nuevos en su ingreso y para las bajas de empleados o contratistas de la empresa. Así como procedimientos de inicio seguro, gestión de contraseñas y acceso seguro a la información.
- Elaborar un procedimiento que permita realizar una trazabilidad del usuario en cuanto a las seguridades de acceso en los diferentes programas y servicios de los sistemas de información.
- Centralizar y definir para las diferentes formas y plantillas que se manejan actualmente en el manejo de seguridades del sistema de información responsables, periodicidad de actualización y hacerlos parte del proceso.

Descripción:
La falta de control de los accesos a la información, los recursos de tratamiento de la información y los procesos de negocio en base a las necesidades de seguridad y de negocio de la organización permite la materialización de potenciales amenazas. Se deben establecer, documentar y revisar con periodicidad la política de control de acceso, teniendo en cuenta los requisitos de la organización para los activos a su alcance. Los usuarios sólo deben tener acceso a la red y a los servicios para los que se les ha autorizado específicamente para usar. El acceso debe ser controlado por un procedimiento de inicio seguro y restringido, de acuerdo con la política de control de acceso. De forma que solamente tengan acceso a la información que necesitan usar o conocer para desarrollar su trabajo.

Motivación:
Corregir problemas y mejorar los resultados del análisis de riesgos. Mejora del anexo 9 - 27001

Controles:
9.1.1 Política de control de acceso
9.1.2 Acceso a las redes y servicios de red
9.2.1 Registro y baja de usuario
9.2.2 Provisión de acceso de usuario
9.2.3 Gestión de privilegios de acceso
9.2.6 Retirada o adaptación de los derechos de acceso9.4.1 Restricción del acceso a la información
9.4.2 Procedimiento de inicio de sesión seguro
9.4.3 Sistema de gestión de contraseñas
9.4.5 Control de acceso al código fuente del programa
Medición:

- Revisión semestral del tiempo transcurrido entre la solicitud y la realización de peticiones de cambio de accesos y número de solicitudes de cambio de acceso cursadas en el semestre anterior.
- Revisión del porcentaje de descripciones de puesto de trabajo que incluyen responsabilidades en seguridad de la información, totalmente documentadas y formalmente aceptadas.

Tiempo: 3 meses
Coste: 1500€

Proyecto 4: Plan de contingencia de datos – Backups y Restores
Responsable de proyecto: Responsable de sistemas
Prioridad: Alta
Activos afectados: Datos
Objetivo:

- Implantar un sistema de copias de seguridad organizado de toda la información con la que se trabaje en la organización.
- Mejora de contingencia de la información de los servidores.
- Reducción del tiempo de restauración de datos.
- Elaborar documentación que permita, en caso de incidente, devolver el sistema al estado previo al incidente.

Descripción:
La información de la organización almacenada en los servidores, en forma de documentación electrónica, bases de datos o desarrollos propios son de alta importancia para la empresa. De forma que se hace necesario desarrollar un correcto plan de copias de seguridad. El trabajador debe procurar en todo momento que los datos relevantes sean almacenados en los servidores de la organización y evitar copias locales. La información debe estar centralizada.
Para los archivos se almacenarán 3 copias: la original y dos copias de seguridad. Cada copia de seguridad será almacenada en lugares diferentes. Una en el servidor interno de la organización y otra en un servicio de nube contratado al efecto.
Las copias de seguridad se realizarán periódicamente. Sobre la información y desarrollos se efectuarán copias de seguridad incrementales cada varias horas, y de los servidores de forma mensual fuera del horario laboral.
Por otra parte, las copias de seguridad deben ser revisadas de forma periódica para asegurar el correcto funcionamiento de estas.
Además, deben documentarse los procedimientos de backups y restores para en caso de incidente se efectúe en el menor tiempo posible la vuelta al estado previo.

Motivación:
Corregir problemas y mejorar los resultados del análisis de riesgos. Mejora del anexo 12 - 27001

Controles:
12.3.1. Copias de seguridad de la información.

Medición:

- Restauración de la información de forma mensual.
- Informe de backups y restores de éxitos y errores.

Tiempo: 3 meses

Coste: 2500€ hardware y software de copias de seguridad
1000€ al año almacenamiento en la nube

Proyecto 5 – Monitoreo SGSI
Responsable de proyecto: Responsable de sistemas.
Prioridad: Media
Activos afectados: Red
Objetivo:

- Instalación de un sistema de monitorización para analizar y ver el estado actual de la red.
- Mejorar la gestión de la red para paliar posibles problemas de la red, dando una visión global de todos los sistemas implicados.
- Comunicación de alertas.
- Medición de ancho de banda y estado de cada enlace de conexión entre máquinas.

Descripción:
Las redes son uno de los elementos más importantes de la empresa. Si la red tiene algún fallo, los datos no llegan a transmitirse o la empresa deja de prestar servicio a los clientes durante el tiempo que dure la caída puede acarrear un grave perjuicio a la organización. Por estas razones, es importante contar con un sistema de monitoreo de red.
Es uno de los principales objetivos asegurar que las redes se encuentren funcionando a pleno rendimiento, el 100% del tiempo. Por lo cual, se debe elegir una herramienta de monitoreo de red adecuada que ayude a detectar posibles problemas antes de que se provoque un colapso o una caída de la red.

Motivación:
Monitoreo y registro de las actividades en la red para establecer medidas correctivas o disciplinarias si es necesario. Mejora del anexo 13 - 27001

Controles:
13.1.1 Controles de Red
13.1.2 Seguridad de los servicios de red

Medición:

- Estadísticas de cortafuegos, tales como porcentaje de paquetes o sesiones salientes que han sido bloqueadas (p. ej., intentos de acceso a páginas web prohibidas; número de ataques potenciales de hacking repelidos, clasificados en insignificantes / preocupantes / críticos).

- Número de incidentes de seguridad de red identificados en el mes anterior, dividido por categorías de leve / importante / grave, con análisis de tendencias y descripción comentada de todo incidente serio y tendencia adversa.

- Porcentaje de intercambio de información, enlaces de terceras partes para los cuales se han definido e implementado satisfactoriamente los requisitos de seguridad de la información.

Tiempo: 3 meses

Coste: 1200€ al año

Proyecto 6 – Concienciación sobre la importancia de la información
Responsable: Área de Recursos Humanos
Prioridad del proyecto: Media
Activos afectados: Personal
Objetivo:

- Establecimiento de medidas de seguridad en el proceso de selección de personal. Incluir en los contratos con los empleados y contratas las obligaciones y responsabilidades ligadas a la Seguridad de la Información.
- Concientizar, educar y capacitar a todos los empleados de la organización en la importancia de la seguridad de la información, sus responsabilidades y las buenas prácticas a seguir para preservar la confidencialidad, integridad y disponibilidad de la información.
- Reducir los riesgos de error humano, comisión de actos ilícitos, uso inadecuado de instalaciones y recursos y manejo no autorizado de la información, junto a la definición de posibles sanciones que se aplicarán en caso de incumplimiento.

Descripción:
La dirección debe velar por la educación e información del personal de la empresa desde su ingreso y en forma continua, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad.
Los empleados realizarán formación y entrenamiento apropiado en las políticas de seguridad y en los procedimientos organizacionales relevantes para la función del trabajo.
Se pondrá a su disposición una serie de recursos sobre cuestiones de seguridad como son manuales, especificaciones, puntos de contacto, etc.
Además, a los empleados se les informará sobre los procedimientos básicos de la seguridad, la importancia del conocimiento y el cumplimiento de las obligaciones y sus responsabilidades en la protección de la información.

Motivación:
Fortalecer el sistema de gestión de la información y contribuir al cumplimiento de la ISO 27001:2013. Mejora del anexo 7 - 27001

Controles:
7.1.1 Investigación de antecedentes
7.1.2 Términos y condiciones de contratación
7.2.1 Responsabilidades de gestión
7.2.2 Concienciación, educación y capacitación en seguridad de la información
7.2.3 Procedimiento disciplinario
7.3.1 Cese o cambio de puesto de trabajo
11.2.8 Equipos de usuario desatendidos
11.2.9 Política de puesto de trabajo despejado y pantalla limpia
12.1.1 Procedimientos operativos documentales

Medición:
Respuesta a las actividades de concienciación en seguridad medidas por (por ejemplo) el número de e-mails y llamadas relativas a iniciativas de concienciación individuales.

Tiempo: La sensibilidad debe ser constante en el tiempo. Para el inicio del proyecto se estima 4 meses.

Coste: 500€

Proyecto 7 – Criptografía
Responsable: Departamento de sistemas
Prioridad del proyecto: Medio
Activos afectados: Datos, Hardware, Servicios
Objetivo:

- Establecer el cifrado de los canales e información de los procesos más críticos de la organización.
- Identificar los activos de información que requieran controles criptográficos y aplicarlos en su proceso.
- Establecer metodologías o canales encriptados para el servicio de correo electrónico.
- Proteger la información sensible que se maneja y transmite.

Descripción:
Con el objeto de asegurar una adecuada protección de la confidencialidad, autenticidad e integridad de la información, es recomendable el uso de sistemas y técnicas criptográficas.

El uso de controles criptográficos o medidas de cifrado se efectuará en base a las políticas definidas. El uso de algoritmos de cifrado y las longitudes de clave deberían ser revisadas periódicamente para aplicar las actualizaciones necesarias en atención a la seguridad requerida y los avances en técnicas de descifrado.

La organización deberá utilizar controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios, para la transmisión de información clasificada y/o para el resguardo de aquella información relevante en atención a los resultados de la evaluación de riesgos realizada por la organización.

Motivación:
Corregir problemas y mejorar los resultados del análisis de riesgos.
Mejora del anexo 10 - 27001

Controles:
10.1.1 Política de uso de los controles criptográficos
10.1.2 Gestión de claves

Medición:

- Porcentaje de sistemas que contienen datos valiosos o sensibles para los cuales se han implantado totalmente controles criptográficos apropiados.

Tiempo: 2 meses

Coste: 1500€

Proyecto 8 – Plan de clasificación de la información y tratamiento del mismo.
Responsable de proyecto: Responsable de sistemas y Dirección.
Prioridad: Media
Activos afectados: Datos, Hardware, Personal
Objetivo:

- Mejorar el tratamiento de los datos almacenados en los servidores y el acceso a los mismos. Cumplimiento de normativas de seguridad y auditoría de acceso a los datos.
- Identificación de los activos, propiedad y responsabilidades sobre los mismos, con el objetivo de proteger adecuadamente cada activo en base al riesgo. Además, de controlar el uso aceptable de ellos, así como su devolución.
- Mejorar la clasificación, etiquetado y manejo de los activos de información.

Descripción:
Efectuar una clasificación de la información basada en distintos niveles de seguridad. Cada usuario y cada área en función de su trabajo y necesidades tendrán acceso solamente a la información que se considere necesaria en el desarrollo de sus funciones. De forma que se efectúe el control de acceso a la información. Especialmente a la categorizada como sensible para la empresa.

Motivación:

Corregir problemas y mejorar los resultados del análisis de riesgos. Mejora del anexo 8 - 27001

Controles:
8.1.1 Inventario de activos
8.1.2 Propiedad de los activos
8.1.3 Uso aceptable de los activos
8.1.4 Retorno de los activos
8.2.1 Directrices de clasificación
8.2.2 Etiquetado y manipulado de la información
8.2.3 Manipulación de activos

Medición:

- Revisión semestral de infracciones en el acceso a la información.
- Revisión anual de permisos de usuarios.
- Revisión anual de la documentación de recursos informáticos.

Tiempo: 3 meses

Coste: 1500€

Proyecto 9: Mantenimiento, control y protección equipos informáticos
Responsable: Responsable de sistemas y dirección
Prioridad del proyecto: Baja
Activos afectados: Hardware – equipos, Aplicaciones
Objetivo:

- Revisar y mejorar la seguridad de los equipos informáticos de la empresa, tales como portátiles, ordenadores de sobremesa y móviles.
- Securización de los ordenadores de los usuarios.

Descripción:
Los dispositivos de uso diario por parte del personal como portátiles, ordenadores de sobremesa y móviles, son susceptibles de sufrir ataques por mal uso, falta de actualizaciones o configuraciones incorrectas.
El objetivo garantizar que la información y las instalaciones de procesamiento de información estén actualizadas y protegidas contra el malware.
Para contrarrestar estos riesgos se procederá a efectuar una serie de acciones como son:
Revisión de la protección ofrecida por el antivirus de uso corporativo.
Configuración centralizada del antivirus con alertas y posibilidad de establecer políticas de uso.
Adquisición de un segundo antivirus con monitorización del uso de los dispositivos.
También se efectuará un control del software instalado en los equipos para garantizar la integridad de los sistemas operacionales de la organización. Y se limitarán los permisos de administrador sobre los equipos al personal de sistemas, restringiendo la posibilidad a los usuarios de instalar software no autorizado.

Motivación:
Corregir problemas y mejorar los resultados del análisis de riesgos.
Mejora del anexo 12 - 27001

Controles:
12.2.1 Controles contra malware
12.6.2 Restricciones de instalación de software
6.2.1 Políticas de dispositivos móviles
11.2.4 Mantenimiento del equipo

Medición:

- Control contra el software malicioso.
- Registros de actividad del administrador y operador del sistema.
- Parcheo vulnerabilidades técnicas de los sistemas de información de manera oportuna.
- Documentación de procedimientos de operación.

Tiempo: 3 meses

Coste: 1500€

Proyecto 10 – Proyecto Desarrollo de software
Responsable: Departamento de sistemas
Prioridad del proyecto: Bajo
Activos afectados: Servicios esenciales, Aplicaciones, Equipos y Comunicaciones.
Objetivo:

- Analizar y elaborar los controles y procedimientos necesarios para el desarrollo de software en el sistema de gestión de la información.
- Definir dentro de la metodología de desarrollo el manejo y control de versiones además de implementar los controles de cambios.
- Efectuar seguimientos en el proceso de desarrollo de software en cuanto a los controles de calidad.
- Definir y documentar como se realiza el desarrollo de las aplicaciones, las metodologías que se utilizan y las buenas prácticas.

Descripción:
El desarrollo del software afecta a diferentes áreas de la empresa por lo que es necesario fijar una herramienta común entre ellas. Debe utilizarse un marco de trabajo para estructurar, planificar y controlar el proceso de desarrollo en los sistemas de información.
Las metodologías de desarrollo de software tienen como objetivo presentar un conjunto de técnicas de modelado de sistemas que permitan desarrollar un software de calidad. Entre los diferentes métodos que existen, debe definirse el que mejor se adapte a la organización y personalizarlo en función de sus necesidades.
Las metodologías de desarrollo favorecen trabajar en equipo de manera organizada. Reducir el nivel de dificultad, organizar las tareas, agilizar los procesos y mejorar el resultado final de las aplicaciones a desarrollar. Evitando problemas, retrasos, errores y, en definitiva, un mal resultado final.

Motivación:
Fortalecer el sistema de gestión de la información y contribuir al cumplimiento de la ISO 27001:2013. Mejora del anexo 14 - 27001

Controles:
14.2.1 Política de desarrollo seguro
14.2.6 Entorno de desarrollo seguro
14.2.7 Externalización del desarrollo de software
14.2.8 Pruebas funcionales de seguridad del sistema
14.2.9 Pruebas de aceptación del sistema

- Pruebas trimestrales de manejo de versiones del software en desarrollo.
- Revisión anual de la metodología de revisión del código en la calidad.
- Revisión anual de la documentación sobre la metodología de desarrollo seguro.

Tiempo: 3 meses

Coste: 1000€

Proyecto 11 – Plan de contingencia y continuidad de negocio
Responsable: Responsable de seguridad y Dirección
Prioridad del proyecto: Bajo
Activos afectados: Servicios esenciales, Aplicaciones, Equipos, Comunicaciones, Elementos auxiliares e Instalaciones.
Objetivo:

- Elaboración de un plan de contingencia y recuperación ante incidentes.
- Definir el método de actuación para minimizar el impacto de las posibles amenazas que afecten al sistema de información de la organización.
- Crear un comité de seguridad que vele por el cumplimiento y continuidad de los procesos.
- Integrar el procedimiento de copias de seguridad en el sistema de información.

Descripción:
Un sistema no puede estar protegido al 100% por lo cual, es importante para la organización definir la estrategia a seguir en caso de que se produzca una incidencia grave y procurar que el impacto sea el menor posible.
Por este motivo, se desarrollará un plan de contingencia y continuidad donde se regularán los mecanismos a poner en marcha en caso de un incidente grave de seguridad. Estos mecanismos ayudarán a mantener el nivel de servicio en unos límites predefinidos, establecerán un periodo de recuperación mínimo, reanudarán la situación inicial anterior al incidente, analizarán los resultados y los motivos del incidente, y evitarán la interrupción de las actividades corporativas.
Se determinarán los procesos y aplicaciones prioritarias a la hora de ser recuperados, así como las estrategias de recuperación para cada uno de los elementos identificados como críticos o que pudieran verse afectados en una contingencia.
Se desarrollará la documentación relacionada con el plan de contingencia:
Plan de crisis (cuyo objetivo es evitar una toma de decisiones improvisada que pueda empeorar la situación o bien que simplemente no se tomen decisiones.), Planes operativos de recuperación de entornos (que deberán especificar sobre qué entorno se aplican.), Procedimientos técnicos de trabajo (se describen las acciones que se han de llevar a la práctica para la gestión y recuperación de un sistema, infraestructura o entorno.)

Motivación:
Evitar las consecuencias de una parada en la actividad diaria de negocio de la empresa.
Mejora del anexo 17 - 27001

Controles:
17.1.1 Planificación de la continuidad de la seguridad de la información
17.1.2 Implementación de la continuidad de la seguridad de la información
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

Medición:

- Planificación e implantación de la continuidad de la seguridad de la información.
- Verificación, revisión y evaluación de la continuidad de la seguridad de la información
- Ejecutar pruebas sobre los entornos identificados.
- Documentar el plan y periodicidad de simulacros que se realizan.
- Registrar los resultados de los simulacros establecidos y sus planes de acción correspondientes.
- Documentar el plan de continuidad de negocio de los servidores redundantes y el tiempo de activación en caso de incidentes.

Tiempo: 3 meses

Coste: 2500€

Proyecto 12 – Procedimiento Gestión de incidentes
Responsable: Responsable de seguridad y Dirección
Prioridad del proyecto: Bajo
Activos afectados: Todos
Objetivo:

- Elaborar las políticas y procedimientos con relación a la gestión de incidentes de seguridad.
- Documentar el plan de respuesta a incidentes y los puntos de contacto para las para la notificación de incidentes, seguimiento y evaluación.
- Asignación y escalado de incidentes (N1 > N2) incluyendo las respuestas de emergencia y la continuidad de negocio.
- Método de recolección de evidencias y pruebas forenses digitales.
- Revisión post-evento de seguridad y procesos de aprendizaje / mejora.

Descripción:
La organización dispone de diferentes tipos de activos de información, cada uno expuesto a sufrir incidentes de seguridad. Resulta necesario contar con un método de gestión de dichos incidentes que permitan comenzar su detección, llevar a cabo su tratamiento y evitar posibles futuros sucesos.
El objetivo de los procedimientos es garantizar que los eventos de seguridad de la información y las debilidades asociadas a los sistemas de información sean comunicados en el tiempo oportuno para que se apliquen las acciones correctivas.
Además, se establecen las responsabilidades y procedimientos para manejar los eventos y debilidades de una manera efectiva. Así como el método de recogida de evidencias para asegurar el cumplimiento de los requisitos legales.
Todo dentro de un proceso de mejora continua para monitorizar, evaluar y gestionar la totalidad de los incidentes en la seguridad de información.

Motivación:
Corregir problemas y mejorar los resultados del análisis de riesgos. Mejora del anexo 16 - 27001

Controles:
16.1.1 Responsabilidades y procedimientos
16.1.2 Informar eventos de seguridad de la información
16.1.3 Informar las debilidades de seguridad de la información
16.1.4 Evaluación y decisión sobre eventos de seguridad de la información
16.1.5 Respuesta a incidentes de seguridad de la información
16.1.7 Recopilación de evidencias

Medición:

- Número y gravedad de incidentes en el último semestre.
- Evaluar los costes de analizar, detener y reparar los incidentes y cualquier pérdida tangible o intangible producida por los incidentes en el último semestre.
- Porcentaje de incidentes de seguridad que han causado costes por encima de umbrales aceptables definidos por la dirección.

Tiempo: 3 meses
Coste: 1000€

PLAN DE EJECUCIÓN

Algunos de los proyectos detallados anteriormente podrían realizarse en paralelo pero se han tenido en cuenta una serie de factores como:

- Coste del programa.
- Gravedad de los riesgos que se afrontan.
- Disponibilidad del personal propio para ejecutar las tareas programadas.

Y buscando optimizar los recursos de la empresa se ha determinado ejecutarlos de forma serial según la prioridad otorgada. Primeramente los proyectos que suponen un mayor impacto para la empresa y después el resto. La planificación está pensada para en el plazo de 3 años cumplir todos los proyectos.

A continuación, se muestra el tiempo planificado para cada proyecto, así como su orden de ejecución.

PROYECTOS	TIEMPO
Proyecto 1 – Definir políticas de seguridad de la información	2 meses
Proyecto 2 – Mejora del CPD	4 meses
Proyecto 3 – Control de acceso	3 meses
Proyecto 4 – Plan de contingencia de datos – Backups y Restores	3 meses
Proyecto 5 – Monitoreo SGSI	3 meses
Proyecto 6 – Concienciación sobre la importancia de la información	4 meses
Proyecto 7 – Criptografía	2 meses
Proyecto 8 – Plan de clasificación de la información y tratamiento del mismo.	3 meses
Proyecto 9 – Mantenimiento, control y protección equipos informáticos	3 meses
Proyecto 10 – Proyecto Desarrollo de software	3 meses
Proyecto 11 – Plan de contingencia y continuidad de negocio	3 meses
Proyecto 12 – Procedimiento Gestión de incidentes	3 meses

Tabla 1. Tiempo estimado proyectos

Seguidamente, mediante un diagrama de Gantt se detalla la planificación de los proyectos.

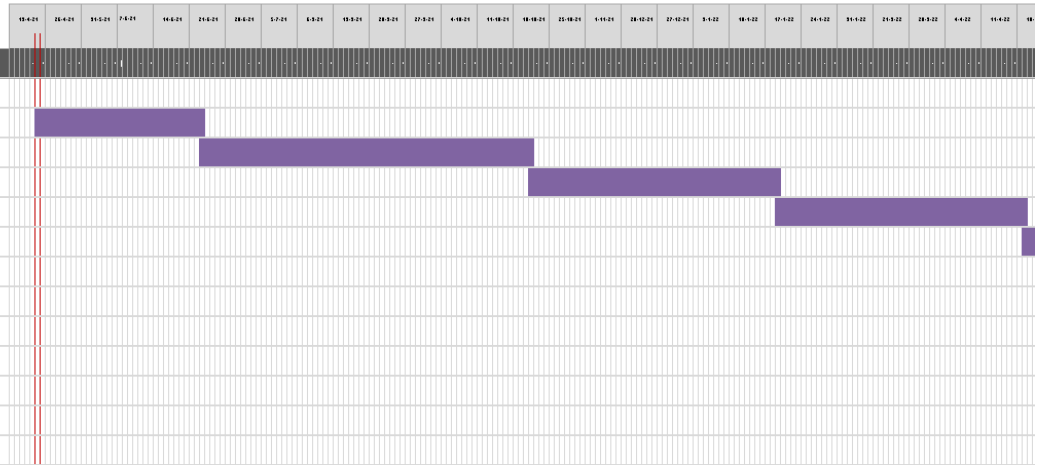
Primer año

SGSI

Natividad García Lacárcel

Inicio del proyecto: sá, 24/4/2021

TAREA	INICIO	FIN
PROYECTOS		
Proyecto 1 – Política de seguridad	24-4-21	23-6-21
Proyecto 2 – Mejora del CPD	23-6-21	21-10-21
Proyecto 3 – Control de acceso	21-10-21	19-1-22
Proyecto 4 – Plan de contingencia de datos – Backups y Rest	19-1-22	19-4-22
Proyecto 5 – Monitoreo SGSI	19-4-22	18-7-22
Proyecto 6 – Concienciación sobre la importancia de la infor	18-7-22	15-11-22
Proyecto 7 – Criptografía	15-11-22	14-1-23
Proyecto 8 – Plan de clasificación de la información y tratam	14-1-23	14-4-23
Proyecto 9 – Mantenimiento, control y protección equipos ir	14-4-23	13-7-23
Proyecto 10 – Proyecto Desarrollo de software	13-7-23	11-10-23
Proyecto 11 – Plan de contingencia y continuidad de negocic	11-10-23	9-1-24
Proyecto 12 – Procedimiento Gestión de incidentes	9-1-24	8-4-24



Planificación proyectos 1

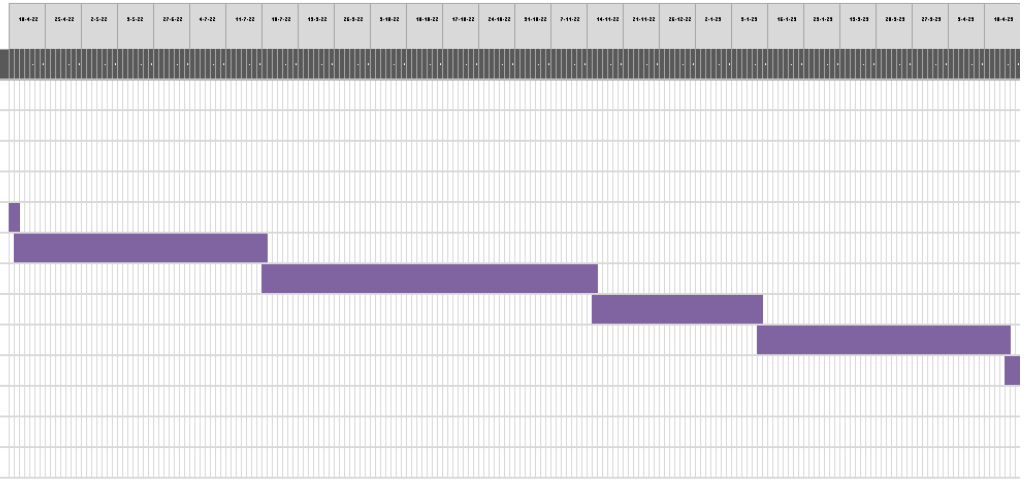
Segundo año

SGSI

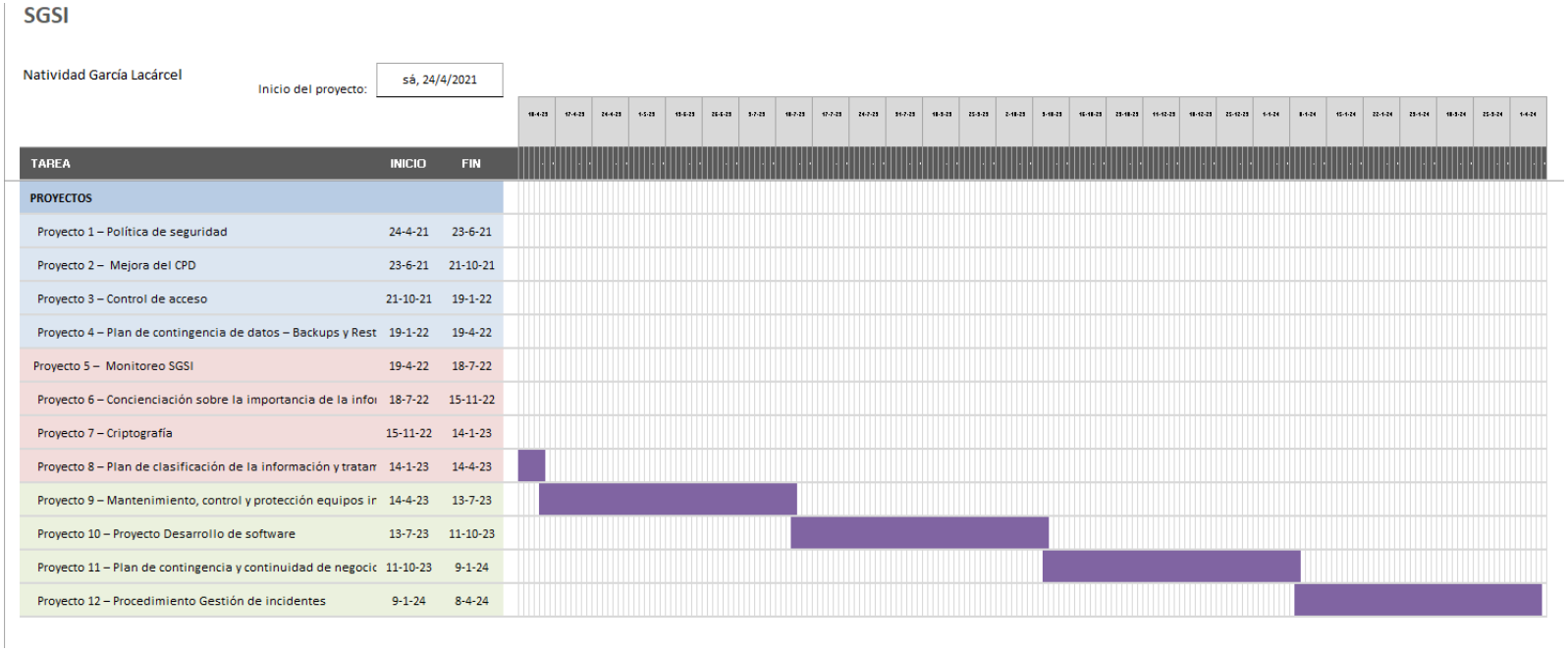
Natividad García Lacárcel

Inicio del proyecto: sá, 24/4/2021

TAREA	INICIO	FIN
PROYECTOS		
Proyecto 1 – Política de seguridad	24-4-21	23-6-21
Proyecto 2 – Mejora del CPD	23-6-21	21-10-21
Proyecto 3 – Control de acceso	21-10-21	19-1-22
Proyecto 4 – Plan de contingencia de datos – Backups y Rest	19-1-22	19-4-22
Proyecto 5 – Monitoreo SGSI	19-4-22	18-7-22
Proyecto 6 – Concienciación sobre la importancia de la infor	18-7-22	15-11-22
Proyecto 7 – Criptografía	15-11-22	14-1-23
Proyecto 8 – Plan de clasificación de la información y tratam	14-1-23	14-4-23
Proyecto 9 – Mantenimiento, control y protección equipos ir	14-4-23	13-7-23
Proyecto 10 – Proyecto Desarrollo de software	13-7-23	11-10-23
Proyecto 11 – Plan de contingencia y continuidad de negocic	11-10-23	9-1-24
Proyecto 12 – Procedimiento Gestión de incidentes	9-1-24	8-4-24



Planificación proyectos 2



Planificación proyectos 3

PRESUPUESTO

A continuación se presenta el resumen del presupuesto de los proyectos por los 3 años:

RESUMEN PRESUPUESTO POR AÑO		
Año 1	Proyectos	Presupuesto
	Proyecto 1	1000€
	Proyecto 2	4000€
	Proyecto 3	1500€
	Proyecto 4	3500€
	Total	10.000€
Año 2	Proyecto 5	1200€
	Proyecto 6	500€
	Proyecto 7	1500€
	Proyecto 8	1500€
	Total	4.700€
Año 3	Proyecto 9	1500€
	Proyecto 10	1000€
	Proyecto 11	2500€
	Proyecto 12	1000€
	Total	6.000€
	TOTAL	20.700€

Presupuesto estimado proyectos