Proyecto CIBERSEGURIDAD EN LAS EMPRESAS

Plan personalizado de implantación

Empresa: xxx

Fecha de emisión del informe:
Asesor/a:

I. INTRODUCCIÓN.

La Cámara de Comercio, Industria y Servicios de Badajoz ha puesto en marcha el Proyecto CIBERSEGURIDAD EN LAS EMPRESAS cofinanciado por la Diputación de Badajoz.

El Programa Ciberseguridad en las empresas tiene como objetivo incentivar el **desarrollo de proyectos en materia de seguridad de la información y la implantación de soluciones en las pymes extremeñas.** Los proyectos apoyados a través de este Programa posibilitan la ampliación y mejora de las capacidades de prevención, detección y corrección ante riesgos cibernéticos.

A partir del análisis de la situación actual, de la pyme evaluada en el diagnóstico, el presente informe definirá y priorizará un conjunto de proyectos en materia de seguridad de la información. El objetivo de la implantación de estos proyectos es la de eliminar o mitigar los riesgos a los que está expuesta la empresa en materia de ciberseguridad.

Con este objetivo, el Proyecto ofrece a las empresas un servicio de acompañamiento y apoyo estructurado en dos fases secuenciales y progresivas:

- **FASE DE DIAGNÓSTICO.**

  En esta fase se plantea la elaboración de un Diagnóstico con el objetivo de evaluar la situación actual de la pyme o el autónomo en materia de ciberseguridad. El análisis tendrá en cuenta aspectos técnicos y organizativos, entre otros. A continuación, se explican las diferentes áreas que se estudiarán:

  - En un primer bloque del proceso de diagnóstico, además de analizar el contexto general de la empresa, se realiza una **evaluación exhaustiva de la infraestructura tecnológica** implantada en la empresa y las características particulares de su utilización (autorización de accesos remotos, características específicas de la empresa en relación con el tratamiento de la información, utilización de servicios corporativos, etc.). Al mismo tiempo, se analizan aspectos específicos de la pyme como son, el **grado de concienciación de la dirección en materia de ciberseguridad**, el conocimiento y la capacitación del conjunto de la empresa, así como, la capacidad de la empresa para llevar cabo proyectos.
    Los aspectos recogidos con anterioridad permiten determinar las necesidades de la pyme en materia de concienciación e implantación de soluciones tecnológicas, también facilita el alineamiento de los proyectos ofertados con los objetivos estratégicos de la empresa y sus necesidades operativas y operacionales. La ciberseguridad es un factor imprescindible dentro del proceso de transformación digital, debiendo abordarse ambos conceptos en paralelo.
  - El siguiente bloque del diagnóstico se centra en la **adopción de procedimientos y soluciones tecnológicas que permitan mitigar o eliminar los riegos asociados al uso de equipos conectados a internet.** Comenzando con la evaluación de la seguridad física de las instalaciones y equipos de la empresa (control de accesos no autorizados, suministro de la energía eléctrica o la realización de tareas de teletrabajo).
  - El siguiente paso es el estudio de las **metodologías utilizadas para garantizar el cumplimiento de buenas prácticas** por parte de los empleados y terceras partes involucradas en el tratamiento de información o la utilización de tecnologías de la información. Después, se analiza la protección de la información transmitida a través de las redes y las medidas adoptadas para minimizar el riesgo.

  El diagnóstico es realizado por un asesor experto específicamente formado a tal efecto, quien es el responsable realizar el análisis del contexto empresarial, tecnológico y de seguridad de la empresa al objeto de ofrecerle recomendaciones y soluciones adaptadas a sus necesidades.

- **FASE DE IMPLANTACIÓN.**

  Tras la realización del diagnóstico, aquellas empresas que deseen acometer la implantación de las soluciones propuestas podrán contar con el apoyo del Programa, que se materializará a través de un apoyo económico dirigido a financiar (en los términos y cuantías previstos) las implantaciones de los proyectos definidos, así como el apoyo del asesor, que tutelará el proceso facilitando la relación con los proveedores tecnológicos y dando seguimiento a los proyectos.

El presente informe es el resultado del diagnóstico realizado a la empresa. En él se recogen los siguientes aspectos:

- Análisis del contexto de la empresa e identificación de las necesidades en materia de ciberseguridad.
- Análisis de aspectos vinculados a la competitividad de la pyme.
- Análisis del grado de seguridad física y del entorno de las instalaciones de la pyme.
- Análisis del grado de seguridad de los equipos y recursos humanos.
- Análisis del grado de seguridad de las operaciones y comunicaciones.

II. ANÁLISIS DEL CONTEXTO GENERAL DE LA EMPRESA

En este capítulo del diagnóstico se estudian las características de la empresa, comenzando por una descripción general de la pyme (dimensión, plantilla, ámbito geográfico...), continuando con un estudio de la Seguridad de los Equipos y Medidas de Protección implantadas, realizando una evaluación del grado de compromiso y concienciación en materia de ciberseguridad y finalizando con un análisis de la Seguridad de las Comunicaciones y Operaciones. A través de este análisis se contextualiza e identifican los focos de actuación prioritarios.

La evaluación de estas áreas lleva implícito un ejercicio de reflexión por parte de las empresas sobre su situación actual y la visión de los objetivos a alcanzar para garantizar la seguridad de la información.

Por otro lado, el análisis del contexto general de la empresa también es utilizado con el objetivo de determinar el grado de compromiso y conocimiento de los dirigentes de la empresa en la ejecución de políticas y proyectos de ciberseguridad.

1. Información General de la empresa

1.1. Identificación de la empresa.

CIF	
Razón Social	
Nombre comercial	
Dirección	
Código postal	
Ciudad	
Teléfono	
Fax	
Página Web	
Sector	
Subsector	
Forma Jurídica	
Nº de empleados	
Año de constitución	

1.2. Persona de contacto.

Persona de contacto	
Teléfono de contacto	
E-mail de contacto	

1.3. Breve descripción de la empresa.

1.4. Empleados.

En la actualidad la empresa cuenta con el siguiente número de empleados:

	0-9
	10-49
	50-249
	250 o más

1.5. Volumen de facturación

El volumen de facturación de una empresa es el conjunto de ingresos realizados en contrapartida de las operaciones de su actividad. En función de dicho volumen, la empresa tendrá unas necesidades de gestión u otras. Así, por ejemplo, una pequeña empresa con una facturación inferior a los 100.000 euros anuales no dispondrá de la misma capacidad de inversión para la implantación de soluciones de ciberseguridad como una empresa de mayor tamaño cuya facturación asciende a más de 1.000.000 euros. De ahí su importancia en este diagnóstico. La facturación de la empresa durante el último año ha sido:

	Menos de 100.000 euros
	Entre 100.000 y 500.000 euros
	Entre 500.001 y 1.000.000 euros
	Entre 1.000.001 y 5.000.000 euros
	Más de 5.000.000 euros

1.6. Estructura organizativa.

La estructura organizativa describe las funciones que tiene asignado cada departamento de la empresa, así como las funciones del personal. Por tanto, la estructura organizativa tiene que ver directamente con la forma en la que la empresa se gestiona, tanto a partir de las estructuras organizativas formales (explicitadas por la dirección) como de las informales (relaciones que surgen en la empresa y no han sido definidas explícitamente). La estructura organizativa de la empresa está formada por las siguientes unidades de gestión:

	Dirección
	Departamento de Administración
	Departamento de Recursos Humanos
	Departamento Comercial y/o Atención al Cliente
	Departamento de Compras
	Departamento de Ingeniería y Diseño
	Departamento de Producción
	Departamento de Calidad
	Departamento de Logística y Distribución

2. Infraestructura tecnológica.

2.1. Tecnologías utilizadas.

Los procedimientos y equipos necesarios para garantizar un nivel adecuado de ciberseguridad, dependen directamente de las tecnologías utilizadas en su operación, debido a que el riesgo a un ciberataque subyace de las acciones realizadas, ¿qué tecnologías utiliza la empresa en sus operaciones?

	Correo electrónico
	Página web corporativa
	Servidores propios
	Plataformas cloud
	Equipos portátiles (móviles, tablets, etc.)
	Ninguna de las anteriores

2.2. Características en el uso de tecnologías IT.

Algunas características intrínsecas a la operativa de las empresas, pueden hacer necesario la utilización de herramientas específicas para su protección. La empresa realiza accesos remotos a servicios corporativos debido a alguna de las siguientes razones:

	La empresa cuenta con varias localizaciones.
	Utiliza redes públicas para la realización de tareas profesionales (cafeterías, aeropuertos, hoteles, etc.).
	Utiliza equipos móviles fuera de las instalaciones.
	Realiza accesos remotos a servicios corporativos (bases de datos, documentos, recursos, etc.).
	Permite acciones de teletrabajo.
	Ninguna de las anteriores

2.3. Proyectos de ciberseguridad.

La empresa tiene previsto realizar acciones para mejorar el nivel de ciberseguridad:

	Sí, en el plazo de los próximos 6 meses.
	Sí, en el próximo año.
	Sí, sin una fecha determinada.
	No existe una partida presupuestaria destinada a implementar acciones de ciberseguridad en los próximos años.

2.4. Implantación de soluciones.

En un entorno como el actual en el que los riesgos cibernéticos aumentan año tras año, no se puede confiar la ciberseguridad de una empresa únicamente en la instalación de software antivirus. El perjuicio de sufrir un ciberataque puede ser alto, por ello, es necesario que las empresas dispongan de un planteamiento y unas políticas de seguridad globales. Las políticas de seguridad deben incluir

medidas proactivas, en las que se adopten buenas prácticas en el uso de las herramientas al alcance de los trabajadores. La empresa ha dispuesto las siguientes herramientas de protección frente a riesgos cibernéticos:

	Todos los equipos corporativos disponen de una herramienta antivirus.
	Todos los equipos corporativos disponen de una herramienta antivirus y la empresa cuenta con un firewall en la red local.
	No se cuenta con un registro de las medidas implantadas en los equipos.
	La instalación de herramientas de protección depende de cada empleado.
	Ninguna de las anteriores

2.5. Desarrollo de la ciberseguridad.

La concienciación de las empresas respecto a la importancia de contar con medidas de protección de la infraestructura IT, ha aumentado en los últimos. Esta tendencia ha potenciado la implantación de herramientas de ciberseguridad, ¿qué tipo de soluciones utiliza o desarrolla la empresa con el objetivo de mejorar su nivel de protección?

	Formación y concienciación de empleados.
	Definición de planes de ciberseguridad.
	Medidas de protección de acceso a redes corporativas.
	Disposición de controles de acceso físico a instalaciones.
	Disposición de controles de acceso lógico.
	Análisis continuo del estado del sistema.
	Implantación de herramientas de protección, actualizadas regularmente.
	No existe un registro de soluciones implantadas, los empleados son responsables de la seguridad de los equipos con los que trabajan.
	Ninguna de las anteriores.

2.6. Autodiagnóstico.

La empresa se identifica con las siguientes afirmaciones:

	La empresa está preparada para mitigar correctamente ciber riesgos, vulnerabilidades y ataques.
	La empresa es capaz de recuperarse fácilmente de un ciberataque.
	Se ha definido el enfoque con el que garantizar la ciberseguridad.
	Ninguna de las anteriores.

2.7. Información.

Identificación de las fuentes de información de ciberseguridad utilizadas en la empresa:

	Medios de comunicación especializados (revistas tecnológicas).
	Páginas webs y foros.

	Expertos externos (consultoría especializada).
	Cursos online, webinars, vídeos.
	Investigación interna.
	Cursos presenciales o talleres.
	Ninguna de las anteriores.

2.8. Colaboradores de ciberseguridad.

Mantener una colaboración con partners especializados en ciberseguridad o participar en foros, es una forma de mejorar el conocimiento sobre las mejores prácticas, obtener información actualizada, asesoramiento especializado o recibir avisos acerca de vulnerabilidades y posibles ataques, entre otras ventajas. Cuál es la participación de la empresa, ¿mantiene contactos con grupos de interés especial u otros foros y asociaciones de ciberseguridad?

	Sí, se han establecido acuerdos de intercambio de información para mejorar la cooperación y coordinación en materia de ciberseguridad.
	Sí, se mantienen relaciones con empresas especializadas en ciberseguridad.
	No, no se mantiene ninguna relación con especialistas en ciberseguridad.

3. Concienciación.

3.1. Riesgos de ciberseguridad.

En algunas ocasiones, las empresas no creen que dispongan de información de interés para los ciberdelincuentes y por ello creen estar libres de sufrir un ataque. Esta percepción suele ser falsa, existen ataques indirectos en los que se busca acceder a listas de contactos y así poder, por ejemplo, realizar spam masivo personalizado o atacar a terceras personas. Otro método de ataque es el de bloquear o encriptar la información, ya que, aunque la información no sea de valor para terceras personas si lo es para la empresa, esta metodología es utilizada por el virus informático tipo ransomware. En su opinión, los mayores riesgos a los que se enfrenta la empresa en relación a la ciberseguridad son:

	Infección de malware en equipos/dispositivos.
	Acceso, compartición, pérdida o robo de datos personales.
	Cesión voluntaria de datos.
	Cesión de información sobre hábitos, tendencias usos de internet.
	Ciberextorsión
	Secuestro de equipos/dispositivos (ransomware).
	Fallo disponibilidad.
	Ninguna de las anteriores.

3.2. Riesgo ciberataques.

La empresa ha sufrido ciberataques o accesos no autorizados a sus servicios corporativos en el último año:

	Sí, ataques graves (poniendo en riesgo la continuidad del negocio).
	Sí, ataques moderados (requirieron la implantación de medidas de contingencia).
	Sí, ataques leves (no supusieron ningún trastorno para la empresa).
	No, no se ha sufrido ningún ciberataque.
	No, no se tienen registros de ciberataques.

3.3. Frecuencia.

La exposición de la empresa a sufrir ciberataques, depende de varios factores como pueden ser: nivel de protección, uso de las redes en su proceso de negocio, conexiones con otros agentes, etc. ¿Con qué frecuencia sufre la empresa incidentes de ciberseguridad?

	Frecuentemente.
	Ocasionalmente.
	Nunca.
	No se lleva un registro de los ciberataques.

3.4. Consecuencias.

El impacto de un ciberataque puede ser muy diverso, ¿cuáles fueron las consecuencias de los ciberataques en la empresa?

	Daño reputacional (pérdida de clientes, ventas, etc.).
	Parada del negocio.
	Costes de recuperación del incidente.
	Sanciones contractuales.
	Ninguna consecuencia.

3.5. Soluciones implantadas.

La empresa dispone de las siguientes soluciones y/o desarrollado los siguientes proyectos:

	Auditoría Técnica de Seguridad.
	Adaptación a la RGPD.
	Auditoría Web y Cumplimiento LSSI-CE.
	Plan de Contingencia y Continuidad.
	Análisis de Vulnerabilidades.
	Certificación Normativa.
	Encriptación de datos.
	Autenticación Multifactor.
	Plataforma de Monitorización de Redes.
	Seguridad de Correo Electrónico.
	Solución Antimalware.
	Control de Aplicaciones (Whitelisting).
	Sistema de Centralización de Certificados.
	Sistema de Alimentación Ininterrumpida (SAI).
	Copias de Seguridad.
	Gestión Centralizada de Dispositivos.
	Sistema SIEM (Security Information and Event Management).
	Hardware Firewall.
	Sistema de Control de Acceso.
	Red VPN.
	Ninguna de las anteriores.

3.6. Necesidades identificadas a priori.

La empresa manifiesta requerir, previamente a la realización del diagnóstico, de la implantación de las siguientes soluciones:

	Auditoría Técnica de Seguridad.

	Adaptación a la RGPD.
	Auditoría Web y Cumplimiento LSSI-CE.
	Plan de Contingencia y Continuidad.
	Análisis de Vulnerabilidades.
	Certificación Normativa.
	Encriptación de datos.
	Autenticación Multifactor.
	Plataforma de Monitorización de Redes.
	Seguridad de Correo Electrónico.
	Solución Antimalware.
	Control de Aplicaciones (Whitelisting).
	Sistema de Centralización de Certificados.
	Sistema de Alimentación Ininterrumpida (SAI).
	Copias de Seguridad.
	Gestión Centralizada de Dispositivos.
	Sistema SIEM (Security Information and Event Management).
	Hardware Firewall.
	Sistema de Control de Acceso.
	Red VPN.
	Ninguna de las anteriores.

3.7. Características soluciones a implantar.

La empresa requiere de las siguientes características en los proyectos de implantación:

	Recabar mejor información de los incidentes de seguridad.
	Soluciones software as a service (SaaS).
	Implantación sencilla.
	Fácil manejo
	Escalables.
	Mejora de la autenticidad y privacidad.
	Aumento de la protección de dispositivos.
	Asequibles.
	Ninguna de las anteriores.

4. Riesgos y medidas de protección.

4.1. Evaluación de riesgos.

La empresa ha evaluado la fortaleza en materia de ciberseguridad del sistema corporativo, realizando las siguientes acciones:

	Se ha realizado una evaluación normativa.
	Se ha realizado un análisis de las vulnerabilidades técnicas a través de test de intrusión.
	Se ha realizado una auditoría técnica de seguridad.
	Ninguna de las anteriores.

4.2. Gestión de vulnerabilidades.

Con el objetivo de reducir los riesgos identificados, ¿se llevan a cabo las siguientes acciones?

	Ante la identificación de vulnerabilidades se estudian los riesgos asociados y las medidas a adoptar.
	Se documenta las características de la vulnerabilidad.
	Se cuenta con una herramienta SIEM, que permite monitorizar de forma continua la red corporativa.
	Se analiza el riesgo de la solución (parches de seguridad, implantación de medidas o equipos de protección).
	Ninguna de las anteriores.

4.3. Detección de eventos de ciberseguridad.

La empresa analiza el tráfico en la red interna:

	Sí, la red es monitorizada con el objetivo de detectar potenciales eventos de ciberseguridad.
	Sí, el entorno físico es monitorizado para detectar potenciales eventos de ciberseguridad.
	Sí, la actividad de los empleados en monitorizada para detectar potenciales eventos de ciberseguridad.
	No, no se dispone de tiempo para detectar potenciales eventos de ciberseguridad.

4.4. Actualización sistema operativo.

Ha establecido los mecanismos necesarios para que los equipos de la empresa realicen automáticamente actualizaciones del sistema operativo.

	Se actualizan los sistemas operativos tan pronto como los parches o actualizaciones están disponibles.
	No, no se toman medidas para mantener actualizados los sistemas.

4.5. Actualización de software.

Es conveniente revisar la existencia de actualizaciones y parches de seguridad de los sistemas instalados en la empresa, además de elaborar procedimientos que permitan la instalación de dichas actualizaciones y parches de forma segura y controlada.

	Existe un protocolo de actualización de software, aplicaciones, bibliotecas y parches de programas.
	Las actualizaciones de software, aplicaciones, bibliotecas y parches de programas son realizadas por personal formado y autorizado por parte de la dirección.
	Las actualizaciones de software son realizadas por los proveedores, según las recomendaciones del fabricante.
	Existe un registro de las actualizaciones de software efectuadas.
	Existe un protocolo de vuelta atrás como medida preventiva antes de introducir cambios en el software.
	Se modifican las aplicaciones informáticas utilizadas en caso de no recibir actualizaciones de seguridad por haber finalizado su ciclo de vida.
	Ninguna de las anteriores.

4.6. Solución antimalware.

El software malicioso (malware) es un tipo de software o contenido web capaz de causar daño en una empresa. Uno de los malware más conocidos es el virus, que infecta a software instalado en un equipo. La empresa ha tomado medidas con el objetivo de prevenir, detectar, controlar y eliminar cualquier software malicioso detectado en los sistemas corporativos:

	Se dispone de una solución antimalware instalada en los servidores corporativos.
	Se dispone de una solución antimalware instalada en todos los equipos con capacidad de conexión a internet (ordenadores, portátiles, tabletas, teléfonos, etc.).
	Únicamente se dispone de una solución antimalware en aquellos dispositivos que almacenan información considerada como sensible para la empresa.
	Se utiliza una solución gratuita con las funcionalidades básicas de seguridad.
	Ninguna de las anteriores.

4.7. Configuración antimalware.

El sistema con el que cuenta la empresa ha sido configurado con alguna de las siguientes funciones:

	Se han analizado las soluciones antimalware previamente a su instalación en la empresa.
	El software antimalware instalado es capaz de realizar análisis en tiempo real.
	Se ha configurado la herramienta antimalware para la realización de análisis y comprobaciones automáticas y periódicas.
	Incluye el análisis de aplicaciones de correo electrónico.
	Dispone de la funcionalidad de control de firmas.
	Ninguna de las anteriores.

4.8. Herramientas antiphishing.

La empresa dispone de una solución con capacidad para proteger a la empresa frente a ataques de phishing:

	Sí, la solución de correo electrónico incorpora un software que identifica correos maliciosos y es capaz de filtrar el correo spam.
	Sí, se cuenta con un sistema antimalware con funcionalidades para la protección del correo electrónico (Antispam, antiphishing, etc.).
	No, no se dispone de ninguna solución específica.

4.9. Calidad del sistema antiphishing.

Se han tomado las siguientes acciones para proteger el correo electrónico corporativo de ataques cibernéticos:

	El software antiphishing cuenta con una funcionalidad sandbox integrada en el correo que analiza automáticamente los archivos adjuntos.
	Se dispone de herramientas de aprendizaje automático que permiten bloquear ataques de phishing.
	Se protege el dominio corporativo por medio de la solución DMARC (Autenticación de mensajes, informes y conformidad basada en dominios).
	Ninguna de las anteriores.

4.10. Técnicas de cifrado.

La utilización de técnicas de cifrado aumenta la protección de la información dificultando el acceso a ella de usuarios no autorizados. La empresa, ¿utiliza técnicas de cifrado?

	Sí, se utilizan técnicas de cifrado de documentos según las condiciones definidas por la empresa.
	Sí, aunque la empresa no ha definido una política de uso.
	No, no se utilizan técnicas de cifrado.

4.11. Política criptográfica.

La empresa ha diseñado una política de uso de las técnicas criptográficas, teniendo en cuenta las siguientes características:

	Se ha identificado la información, que, por su criticidad para la empresa, debe ser salvaguardada con técnicas criptográficas.
	Se ha realizado una evaluación de riesgos con el objetivo de fijar los niveles de protección (tipo, fortaleza y calidad del algoritmo de cifrado) del sistema de cifrado.
	Se han establecido responsables de implantación y gestión de la política de cifrado.
	Se ha definido un protocolo de renovación de los algoritmos y claves del sistema de cifrado.
	Se utilizan técnicas de cifrado en información sensible transportada a través de dispositivos móviles o extraíbles o a través de líneas de comunicación.
	Ninguna de las anteriores.

4.12. Claves de cifrado.

Mecanismos para la gestión del uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida en la empresa.

	Las claves generadas se modifican para distintos sistemas criptográficos y diferentes aplicaciones.
	Se cuentan con mecanismos para la gestión de claves de cifrado, incluyendo medidas para su salvaguarda.
	Ninguna de las anteriores.

4.13. Soluciones de cifrado.

El cifrado puede afectar a diferentes niveles del almacenamiento de la información. Es posible realizar cifrado a nivel de documento o utilizar estas técnicas en el conjunto del disco de un equipo. La empresa utiliza las técnicas criptográficas como medida de protección de los siguientes sistemas:

	Cifrado de disco.
	Cifrado de carpetas.
	Cifrado de documentos.
	Ninguna de las anteriores.

4.14. Utilización de copias de seguridad.

Las empresas deben pensar acerca del valor crítico de la información para su negocio, información de clientes, pedidos, presupuestos, o detalles de facturas, por ejemplo. La vulneración de esta información, en un caso extremo, puede poner en peligro la continuidad del negocio para algunas organizaciones. Todas las empresas, independientemente de su tamaño, deben realizar periódicas copias de seguridad de la información crítica almacenada, y estar seguros de que estas copias pueden estar disponibles en tiempos adecuados. A través de esta acción, las empresas están poniendo en marcha una medida que permitirá a la empresa continuar con el normal funcionamiento ante el impacto de un incidente de ciberseguridad. Además, gracias a un sistema de copias de seguridad con rápida capacidad de recuperación evita que la empresa se vea afectada por la extorsión de ciberataques como el denominado ransomware. La empresa sigue las siguientes pautas:

	Se realizan copias de seguridad.
	Se ha identificado aquellos activos imprescindibles para la empresa y de los cuáles se deben realizar copias de seguridad (inventariado).
	Se ha definido un responsable encargado de realizar copias de seguridad.
	Se lleva a cabo un control de los soportes utilizados para realizar las copias de seguridad.
	Se ha establecido un procedimiento para la realización de copias de seguridad, su restauración y destrucción.
	Ninguna de las anteriores.

4.15. Procedimiento de copias de seguridad.

Las empresas deben elaborar y aplicar procedimientos en los que se describa la forma de realizar las copias, su restauración y borrado. De esta forma se facilita la recuperación de la información en caso de incidente y se asegura el buen uso:

	Se mantiene un registro preciso y completo de las copias de seguridad.
	Se especifica la frecuencia de realización de las copias de seguridad.
	Las copias de seguridad están almacenadas en un emplazamiento alejado del emplazamiento principal.
	Se realizan comprobaciones de la respuesta de los soportes de almacenamiento periódicamente.
	Las copias de seguridad son protegidas mediante técnicas de cifrado en caso de ser almacenadas en sistemas en plataformas cloud.
	Ninguna de las anteriores.

4.16. Frecuencia realización copias de seguridad.

La frecuencia con la que se realizan las copias de seguridad dependerá de distintos factores como son: la variación de los datos generados, el coste del almacenamiento y las obligaciones legales pertinentes. Buena parte de las herramientas disponibles con el fin de realizar copias de seguridad ofrecen la posibilidad de realizarlas de forma automática. Es recomendable utilizar estas funciones, ya que, además de ahorrar tiempo es un mecanismo que permite asegurar que se han realizado copias de seguridad de la última versión de los documentos. La empresa realiza copias de seguridad con frecuencia:

	Varias veces al día.
	Diariamente.
	Semanalmente.
	Mensualmente.
	Nunca.

5. Comunicación de operaciones.

5.1. Procedimiento de operación.

La elaboración de procedimientos de operación es un instrumento vital, estos deben ser puestos a disposición de aquellos trabajadores afectados. Esta medida facilita que el personal adopte un código de buenas prácticas y disponga de información de consulta ante dudas en la realización de sus tareas. La empresa ha elaborado procedimientos para los siguientes aspectos:

	Encendido y apagado de ordenadores.
	Copias de seguridad.
	Mantenimiento de los equipos.
	Gestión de soportes de almacenamiento.
	Gestión de acceso a entornos con equipos de tratamiento de datos.
	Gestión del correo electrónico.
	Procedimientos de seguridad para la certificación ISO 27001.
	Ninguna de las anteriores.

5.2. Procedimiento de actuación frente a incidentes.

Los incidentes de ciberseguridad pueden suponer grandes daños para las empresas, algunas de las consecuencias pueden ser el espionaje, el robo o destrucción de datos. Para evitar o limitar estos daños, es necesario contar con una metodología de gestión que establezca la forma de procesar eficientemente estos eventos. Cómo actúa la empresa ante un incidente de ciberseguridad, ¿ha definido el procedimiento de actuación ante incidentes?

	La empresa cuenta con un procedimiento siendo este probado, por el que se notifican los incidentes a la autoridad competente.
	No se ha desarrollado un procedimiento.

5.3. Gestión de incidentes.

La protección total ante incidentes de ciberseguridad no existe, siempre hay posibilidades de que estos eventos se produzcan. En consecuencia, se debe planificar un plan de acción en el que se detalle la forma de actuar, las personas involucradas, responsabilidades, canales de comunicación, etc. Todos los miembros de la empresa deben conocer y ser capaces de aplicar el procedimiento definido, con este propósito la empresa ha establecido:

	Se ha seleccionado una persona responsable de la gestión de incidentes de ciberseguridad.
	Se ha definido un punto de contacto en la empresa para la detección y comunicación de incidentes de seguridad.
	Se ha definido el procedimiento de comunicación ante incidentes de seguridad de la información.
	Se ha establecido un proceso de retroalimentación para comunicar a los usuarios la resolución de incidencias.
	Ninguna de las anteriores.

5.4. Respuesta ante incidentes.

El procedimiento de respuesta debe estar documentado, incluye las siguientes acciones:

	Se realiza una recogida de pruebas tras la comunicación del incidente.
	Se realiza un análisis forense de las evidencias recogidas.
	Se informa a todo el personal afectado por el incidente tanto interno como externo a la empresa.
	Se toman medidas para mejorar puntos de debilidad que pudieran causar o contribuir al incidente.
	Existe un protocolo de cierre y registro del incidente una vez haya sido tratado.
	Se ha diseñado un plan de continuidad.
	Ninguna de las anteriores.

5.5. Plan de contingencias.

El plan de contingencia ante incidentes debe incluir las acciones que deben realizar los empleados para devolver a la normalidad a los procesos de negocio después de producirse un incidente de ciberseguridad. La empresa ha definido:

	Se dispone de un plan de contingencia con una lista de pasos claros y entendibles.
	Se dispone de un plan de contingencia, pero las acciones están definidas de forma no clara o vaga.
	No se dispone de un plan de contingencia.

5.6. Actuaciones posteriores.

La empresa ha llevado a cabo alguna de las siguientes acciones, ante el impacto de un ciberataque:

	La empresa ha tomado medidas para que los eventos de ciberseguridad producidos en el pasado no vuelvan a ocurrir.
	Se han realizado cambios, pero no se ha encontrado la causa del incidente.
	No se han realizado cambios en el sistema una vez ocurrido el incidente de ciberseguridad.

5.7. Gestión de redes.

Con el objetivo de asegurar la protección de la información en las redes y los equipos de tratamiento de la información. La empresa ha adoptado las siguientes medidas con el objetivo de gestionar la seguridad de redes:

	Ha definido la responsabilidad y el procedimiento para la gestión de equipos de red.
	Se cuenta con una herramienta de monitorización del uso de servicios de red.
	Ninguna de las anteriores.

5.8. Segmentación de redes.

La segmentación de la red aumenta el nivel de protección incorporando capas de seguridad internas, lo que dificulta la expansión de ataques cibernéticos. En relación a este aspecto es considerado una buena práctica la segregación en diferentes redes de: Servicios de información; Usuarios y Sistemas de información. En este sentido, la empresa ha llevado a cabo las siguientes acciones:

	La red corporativa esta segmentada a través de un dispositivo de filtrado (firewall).
	La red corporativa esta segmentada por el dispositivo de acceso a la red (router).
	Se cuenta con una red DMZ.
	La red corporativa no está segmentada.

5.9. Acceso remoto.

La empresa habilita el acceso remoto a la red corporativa, permitiendo la utilización de recursos (información, servicios).

	Sí, de forma permanente.
	Si, pero los empleados no disponen de acceso a información sensible o crítica desde localizaciones remotas.
	No, no se permite el acceso remoto a ningún archivo o documento de la empresa.

5.10. Seguridad servicios de red.

Las empresas deben contar con empresas proveedoras de servicios de red que garanticen unas condiciones de seguridad adecuadas a los requisitos de la empresa. A este respecto la empresa ha contratado el siguiente servicio de seguridad con el proveedor de servicios de red:

	Sistemas de detección de intrusiones (IDS).
	Ninguna de las anteriores.

5.11. Redes externas.

En ocasiones los trabajadores se ven obligados a hacer uso de redes externas a las corporativas con fines profesionales, como consecuencia de viajes, reuniones, teletrabajo, etc. Se debe asumir, por prudencia, que las redes externas disponen de un nivel de seguridad bajo exponiendo las comunicaciones y datos transmitidas por ellas a accesos no autorizados. El uso de redes inalámbricas externas a la empresa debe quedar limitado y no se debe hacer uso de ellas si no existen garantías de que la información transmitida está lo suficientemente protegida.

	Se establece las condiciones necesarias para la utilización de la red (contraseña privada, acceso limitado, protocolo WPA2, acceso a portales con protocolos de seguridad https://, etc.).
	Se ha incorporado una Red Privada Virtual (VPN).
	Ninguna de las anteriores.

5.12. Disposición firewall.

Los firewalls son herramientas que permiten detener accesos fraudulentos o no autorizados a las redes y servicios corporativos. Estos sistemas son básicos en la actualidad, debido a la interconexión de los equipos corporativos. La empresa ha establecido las siguientes medidas:

	Se dispone de un hardware firewall en la red interna de la empresa que protege la infraestructura corporativa.
	Se utilizan software de firewall instalados en los equipos de usuario.
	Se utilizan ambos sistemas de firewall (hardware y software).
	No, no se dispone de ninguna protección que limite la entrada a la red corporativa.

5.13. Configuración firewall.

La empresa ha realizado modificaciones en la configuración del firewall, siguiendo las siguientes medidas:

	La contraseña por defecto de administración del firewall se ha modificado siguiendo pautas para la generación de contraseñas robustas.
	Las conexiones abiertas (permitida por puertos o servicios) en los firewalls solo se realizan tras recibir autorización.
	La utilización de servicios vulnerables, como puede ser: NetBIOS, Telnet, TFTP, RPC, rlogin, rsh o rexec, han sido deshabilitados o bloqueados por defecto y solo son habilitados bajo autorización.
	Las reglas del sistema firewall inutilizadas han sido eliminadas o deshabilitadas.
	Realiza una revisión periódica del sistema firewall.
	Ninguna de las anteriores.

5.14. Configuración red Wifi.

El objetivo de establecer una configuración de la red WiFi corporativa es mantener un sistema seguro, rápido y estable. Los medios utilizados para este fin no deben dificultar la utilización de la red. La empresa ha tomado las siguientes medidas para aportar seguridad a la red inalámbrica corporativa:

	Se ha realizado con el objetivo de minimizar la cobertura fuera de los espacios de control de la empresa.
	Se ha establecido una configuración de seguridad de la infraestructura inalámbrica.
	Se despliega automáticamente la configuración de seguridad corporativa en los dispositivos conectados a la red.
	Se detectan cambios no autorizados en la configuración de seguridad de los dispositivos conectados a la red.
	Se verifican las configuraciones de seguridad y se modifican en caso de detección de vulnerabilidades.
	Se ha segmentado la red WiFi estableciendo una red exclusiva para invitados.
	Ninguna de las anteriores

5.15. Configuración del punto de acceso (router).

Con el objetivo de mejorar el nivel de seguridad en las redes inalámbricas se han tomado las siguientes medidas de seguridad en la configuración del punto de acceso de la red WiFi:

	Se ha modificado el nombre de la red WiFi o SSID.

	Se ha modificado la contraseña predefinida por el proveedor de acceso a la red WiFi.
	Se mantiene actualizado el firmware del router.
	Se ha configurado la red WiFi con cifrado WEP.
	Se ha configurado la red WiFi con cifrado WPA2 o WPA3.
	Se ha desactivado el sistema WPS (WiFi Protected Setup).
	Ninguna de las anteriores.

5.16. Gestión de acceso de usuario.

Una adecuada gestión de acceso a los usuarios debería garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.

	Se han definido grupos de usuarios en función del tipo de información al que podrán acceder.
	Se limita la capacidad de modificación de la información a la que tienen acceso los empleados.
	Se ha definido un procedimiento para dar de alta/baja los permisos de los usuarios.
	Se realiza revisiones de los permisos concedidos.
	Ninguna de las anteriores.

5.17. Procedimiento de inicio de sesión.

El protocolo de inicio de sesión, cuenta con las siguientes características:

	Muestra un aviso general en el que se advierte de que el acceso únicamente se debe realizar por personal autorizado.
	No existen medidas de asistencia en el proceso, que puedan facilitar el acceso de personal no autorizado.
	Genera un evento de seguridad cuando se detecta un intento potencial o con éxito de violación de los controles de inicio de sesión.
	Muestra información tras completar con éxito el inicio de sesión: fecha y hora del anterior inicio de sesión con éxito; detalles de cualquier intento de inicio de sesión sin éxito desde el anterior con éxito.
	Ninguna de las anteriores.

5.18. Autenticación.

Controlar el acceso a los sistemas y aplicaciones corporativas es un hecho que la mayor parte de las empresas ya realizan. En la actualidad, el sistema de control más extendido es aquel que empareja usuario/contraseña para la identificación de los usuarios. En ocasiones en las que se accede a servicios críticos o se realizan operaciones confidenciales para las empresas este sistema proporciona unas garantías de seguridad demasiado bajos para el entorno en el que trabajamos. La ciberdelincuencia evoluciona rápidamente y las empresas han de adaptarse. La empresa utiliza alguno de los siguientes sistemas de autenticación para el acceso a los sistemas, aplicaciones o servicios corporativos:

	Mecanismo basado en usuario/contraseña.

	Autenticación por medio de tokens.
	Autenticación biométrica.
	Autenticación por medio de 2 factores.
	Ninguna de las anteriores.

5.19. Gestión privilegios de acceso.

La concesión de privilegios de acceso se debe de realizar de forma controlada y restringida, alineando el procedimiento con la política de control de acceso. Se siguen los siguientes pasos a la hora de gestionar los privilegios de acceso:

	Estudio de los derechos de acceso privilegiados asociados a cada sistema o proceso junto con los usuarios a los que hay que asignarlos.
	Asignación de derechos basada en los requisitos mínimos para el desempeño de funciones.
	Ninguna de las anteriores.

5.20. Gestor de correo electrónico.

Existen diferentes herramientas que ofrecen servicios de correo electrónico, la empresa ha optado por:

	Plataforma de correo electrónico gratuito (Gmail, Yahoo, etc.).
	Dispone de un servidor propio de correo electrónico.
	Se ha subcontratado los servicios de correo electrónico.

5.21. Procedimiento correo electrónico.

La amplia utilización de esta herramienta en el mundo empresarial la ha convertido en el foco de muchos ciberdelincuentes siendo uno de los medios más utilizados para perpetrar sus ataques. Es habitual encontrarse en buzones de correo corporativo con mensajes spam o correos de phishing que utilizando técnicas de ingeniería social buscan engañar al receptor para conseguir el robo de credenciales, datos confidenciales o infectar los equipos. Con el objetivo de prevenir los riesgos procedentes de la utilización de esta herramienta de comunicación corporativa se deben impulsar medidas de concienciación y formación a los empleados para el buen uso del correo y poner a su disposición normas que regulen las condiciones y circunstancias de utilización, así como las posibles sanciones ante malas prácticas. La empresa ha establecido una normativa de uso permitido y seguro del correo electrónico corporativo que previene de cometer errores, incidentes y usos ilícitos, además de evitar ataques por este canal:

	Se ha definido una normativa en la que se establece el uso del correo electrónico corporativo que es aceptada por los empleados.
	Las cuentas de correo electrónico corporativas no son publicadas en páginas web o redes sociales sin la utilización de técnicas de ofuscación.
	Se prohíbe el uso del correo corporativo con fines personales y fuera de las normas establecidas por la empresa.
	Se cuenta con un sistema de control de acceso al correo electrónico corporativo.
	Ninguna de las anteriores.

5.22. Certificados digitales.

La utilización de documentación digital es una práctica que se ha ido instaurando en las empresas, siendo en la actualidad su uso generalizado con independencia del tamaño y actividad estas. Digitalizar la documentación trae consigo algunas necesidades, como el hecho de garantizar la autenticidad, integridad y no repudio. Estos aspectos pueden ser resueltos a través de la utilización de certificados digitales. La empresa, ha tomado las siguientes medidas:

	Se cuenta con un certificado electrónico de persona jurídica.
	Se cuenta con un certificado electrónico de pertenencia a empresa.
	Se cuenta con un certificado electrónico de representante.
	Se cuenta con un certificado electrónico de factura electrónica.
	No se cuenta con ningún método de certificación de documentos digitales.

5.23. Utilización de certificados digitales.

La utilización de los certificados digitales es imprescindible en aquellos escenarios en los que se desea garantizar la autenticidad y el no repudio de la información. La empresa emplea los certificados digitales en los siguientes casos:

	Tramitación con Administraciones Públicas.
	Elaboración de facturas.
	Autenticación y sellado en el tiempo para aumentar la confiabilidad.
	Ninguna de las anteriores.

5.24. Dispositivo de almacenamiento de certificado.

	Se administran los certificados digitales a través de un fichero instalado en equipo de usuario.
	Se administran los certificados digitales a través de la utilización de tarjetas.
	Se administran los certificados digitales a través de la utilización de tokens.
	Se dispone de una plataforma para la gestión de certificados digitales.
	Ninguna de las anteriores.

III. IMPLANTACIÓN DE SOLUCIONES.

Tras la realización del diagnóstico, aquellas empresas que deseen acometer la implantación de las soluciones propuestas podrán contar con el apoyo del Programa, que se materializará a través de un apoyo económico dirigido a financiar (en los términos y cuantías previstos) las implantaciones de los proyectos definidos, así como el apoyo del asesor experto, que tutelará el proceso facilitando la relación con los proveedores tecnológicos y dando seguimiento a los proyectos.

A partir del análisis de la situación actual, de la pyme evaluada en el diagnóstico, se definirá y priorizará un conjunto de proyectos en materia de seguridad de la información. El objetivo de la implantación de estos proyectos es la de eliminar o mitigar los riesgos a los que está expuesta la empresa en materia de ciberseguridad.

De este modo, a la actual empresa se le implantará las soluciones que en materia de ciberseguridad son las aconsejadas según el estudio y análisis anterior para conseguir los objetivos propuestos.

FICHA DE SOLUCIÓN IMPLEMENTADA

(Incluir una ficha por cada solución implantada en la empresa)

Denominación de la solución	
Duración de la implantación	
Descripción de las actividades realizadas y servicios prestados	
Detalle de la solución implantada y sus características	
Impacto esperado en la empresa	
Incidencias o problemáticas detectadas durante la implantación de la solución	
Desviaciones producidas respecto a la propuesta inicial	

COSTE DEL PROYECTO (incluir las líneas necesarias)

Concepto del gasto	Proveedor	Fecha gasto	Importe (€)
			0,00€
			0,00€
			0,00€
			0,00€
			0,00€
		TOTAL	**0,00€**

Fdo.: _____
Por la empresa

Fdo.: _____
Asesor/a