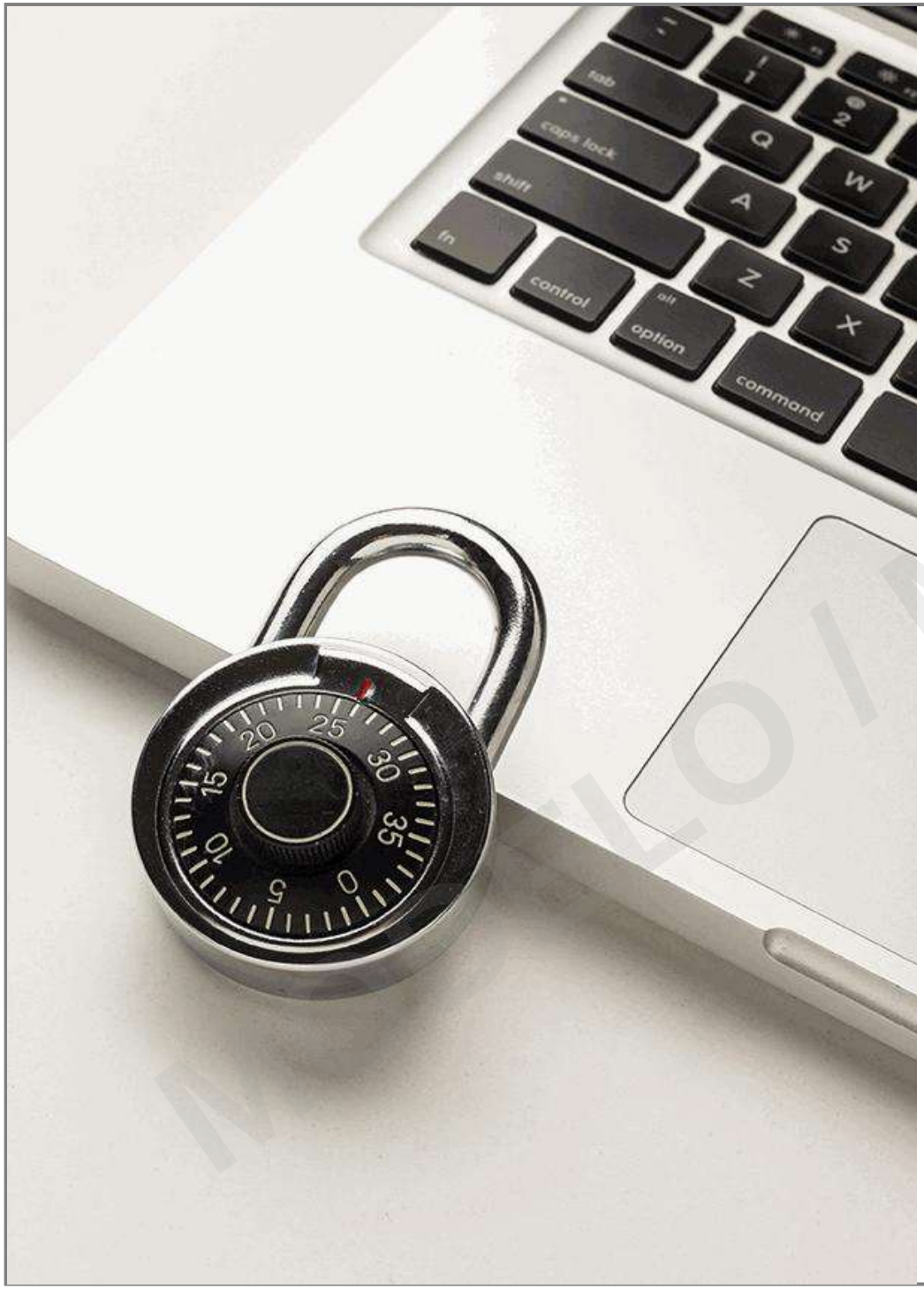


INFORME DE GESTIÓN DE CIBERRIESGOS

EMPRESA XXX

6 de julio de 2022

CONTENIDO

1. CONTROL DE CAMBIOS

REGISTRO DE VERSIONES:

FECHA	VERSIÓN	REVISIÓN	RESPONSABLE (Interno)	DESCRIPCIÓN CAMBIOS
06/07/2022	v1.0		Jesus	

ELABORADO POR:

	RESPONSABLE	CARGO
JESUS CANOVACA	Jesus Canovaca	Gerente

2. IDENTIFICACIÓN DE LA EMPRESA

EMPRESA XXX , con CIF **V...** pertenece al sector de **AGROALIMENTARIO** y su actividad CNAE es: **4631**.
Su ubicación principal sita en

[redacted]

3. INTRODUCCIÓN Y OBJETIVOS

La ciberseguridad se ha convertido en una realidad para las Pequeñas y Medianas Empresas. En la actualidad las amenazas han penetrado en este tipo de empresas, a medida que crece su importancia en la cadena de valor económico y se convierten en parte de la economía digital.

Uno de los principales desafíos para **EMPRESA XXX** es reconocer que el departamento de IT y de sistemas debe evolucionar. Las limitaciones presupuestarias de las pymes son su punto débil, y los piratas informáticos lo saben. Si bien las herramientas como un antivirus o un firewall básico pueden ofrecer cierto grado de seguridad, las PYMES deben personalizar los controles de seguridad y reevaluarlos de forma continua.

A medida que cambia el panorama digital para **EMPRESA XXX**, también cambia el panorama de la inseguridad cibernética.

En ese sentido, el presente análisis riesgos informáticos y de ciberseguridad realizado sobre **EMPRESA XXX** le ofrece los siguientes beneficios:

Por una parte, convivan y se organizan en relación con la toma de decisiones [illegible] comerciales, financieras, laborales, que les garanticen alcanzar los resultados previstos. Por otra, se enfrentan a los riesgos fortuitos que pueden alterar los recursos y sus planes de acción, riesgos que de manera **accidental o brusca pueden afectar a la seguridad y salud** de las personas que trabajan en las empresas, al **patrimonio de las mismas**, a sus responsabilidades y a la propia [illegible], poniendo en peligro la continuidad del proyecto empresarial.

En ese sentido, se encuentran aspectos tan característicos como:

Dispondrá de una **visión precisa de los activos** relacionados con la información de la empresa.
Conocerá los **riesgos a los que se expone** la empresa.
Podrá **medir el impacto** que produciría en la empresa [illegible].
Facilita la toma de decisiones [illegible] en ciberseguridad y reduce los tiempos ante posibles incidentes de seguridad.
Ayuda a elegir la **mejor alternativa** en cuanto a **métodos de reducción** de los riesgos.
Permite realizar una **evaluación de los resultados**, para implementar mejoras o reforzar aspectos débiles en las medidas de seguridad.
Garantiza la continuidad del negocio, disponiendo de planes y protocolos [illegible] graves.
Ayuda a crear una **cultura de prevención en la empresa**, involucrando a todas las personas que la forman.

3. INTRODUCCIÓN Y OBJETIVOS

Ante este horizonte, **JESUS CANOVACA** proporciona a **EMPRESA XXX** una primera toma de contacto con la metodología de gestión de **ciberriesgos** informándole sobre las distintas medidas de control y soluciones aseguradoras que constituyen una respuesta eficaz ante los riesgos y facilitándole la información de partida necesaria para desarrollar su actividad en el marco de la gestión de riesgos adaptada a un entorno **tecnológico** cambiante.

EMPRESA XXX, a través del presente análisis de riesgos, dispondrá de la **información de partida** necesaria para desarrollar su actividad en el marco de la gestión de riesgos y adaptarse a un entorno **tecnológico** cambiante; afrontando la gestión de manera global y adaptada a las circunstancias de cada momento.

Como parte de este análisis, se identifican las actividades o áreas más vulnerables dentro de **EMPRESA XXX**, evaluando los factores que puedan significarse como determinantes a la hora de una eventual materialización de un riesgo o amenaza cibernética y minimizando en el tiempo la probabilidad e impacto de los riesgos a los que se enfrenta.

Con carácter general, los ciberriesgos a los que se enfrentan todas las empresas incluidos en presente análisis, pueden agruparse en cuatro áreas clave que impactan directamente en las actividades empresariales sien[illegible] estos ampliables de acuerdo con las necesidades de cada empresa y [illegible] gestión activa de riesgos y mejora continua:

1. **Ciberriesgos derivados de la organización interna de la empresa.**
2. **Ciberriesgos derivados de la tecnología que utiliza la empresa.**
3. **Ciberriesgos derivados de Terceras Partes [illegible]**
4. **Ciberriesgos derivados de medidas de seguridad implantadas en la empresa.**

Como primera fase del proyecto, se elabora un **SISTEMA EFICAZ DE LA GESTIÓN DE RIESGOS** en el presente Informe de Análisis de Riesgos identificando los principales ciberriesgos a los que está expuesta **EMPRESA XXX**, su nivel actual de cobertura a través de las distintas medidas de control que tiene establecidas y una propuesta de medidas de control a establecer para reducir la probabilidad e impacto en caso de ocurrir.

4. IDENTIFICACIÓN DE RIESGOS

CUESTIONARIOS DE IDENTIFICACIÓN DE RIESGOS

La identificación de los riesgos, su monitorización y seguimiento es relevante para el control de los mismos. Por ello, **JESUS CANOVACA**, a través de un sistema de identificación de riesgos basado en la realización de cuestionarios a los distintos implicados en los procesos de la empresa, le ofrece a **EMPRESA XXX** un detalle de todos aquellos ciberriesgos susceptibles de ser materializados en la empresa y una valoración inicial de probabilidad de ocurrencia e impacto en la materialización en base a la experiencia propia de la empresa o de su sector.

Los cuestionarios realizados a distintos miembros de **EMPRESA XXX** están basados en una estructura de riesgos y medidas de gestión definida previamente por **JESUS CANOVACA.**

La identificación de riesgos y medidas se ha basado en la siguiente distribución de bloques:

CLASE	CATEGORÍA	RIESGO
CIBERRIESGO	Organización Interna	ACCESOS INDEBIDOS
		DEPENDENCIA TECNOLÓGICA
		INCORRECTA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
		INCORRECTA SELECCIÓN Y FORMACIÓN Y COMPROMISO DEL PERSONAL
	Seguridad	INCIDENTES DE SEGURIDAD REACIONADOS CON EL ENTORNO DE LA EMPRESA
		INCIDENTES RELACIONADOS CON EL ACCESO A LOS DATOS (COPIAS DE SEGURIDAD DE DATOS)
		INCIDENTES/BRECHAS DE SEGURIDAD
		INCORRECTA GESTIÓN DE CONTRASEÑAS
		PÉRDIDA DE CONFIDENCIALIDAD DISPONIBILIDAD E INTEGRIDAD DE LOS DATOS PERSONALES
		RESILIENCIA Y CONTINUIDAD DEL NEGOCIO
	Tecnología	DAÑOS EN EL SISTEMA INFORMATICO O EN LOS ACTIVOS DE SU EMPRESA DERIVADOS DEL USO DE HARDWARE.
		DAÑOS EN EL SISTEMA INFORMATICO O EN LOS ACTIVOS DE SU EMPRESA DERIVADOS DEL USO DE REDES DE TELECOMUNICACIONES
		DAÑOS EN EL SISTEMA INFORMATICO O LA RED DE LA EMPRESA DERIVADOS DEL USO DE DISPOSITIVOS MOVILES
		DAÑOS EN EL SISTEMA INFORMATICO O LA PERDIDA DE LA EMPRESA DERIVADOS DEL USO DE SOFTWARE
	Terceras partes	INCORRECTO FUNCIONAMIENTO DE LA EXTERNALIZACION DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y CLOUD COMPUTING
		INCORRECTO FUNCIONAMIENTO DE SERVICIOS EXTERNALIZADOS

Cada uno de los grandes bloques señalados se ha distribuido en dos niveles de cuestionarios:

IDENTIFICACIÓN DE RIESGOS: nos ayudan a identificar los distintos ciberriesgos a los que puede enfrentarse la empresa

IDENTIFICACIÓN DE CONTROLES: Nos ayudan a identificar las medias de gestión del riesgo que actualmente dispone la compañía así como aquellas que deberían tenerse y que en la actualidad la empresa no tiene implantadas**.**

El resumen total de los trabajos de identificación de riesgos y controles realizado es el siguiente:

TIPO	CUESTIONARIO	Nº PREGUNTAS REALIZADAS	MIEMBROS DE LA EMPRESA ENCUESTADOS
RIESGOS	RIESGOS CIBER	67	1
MEDIDAS DE CONTROL	CONTROLES CIBERRIESGO	33	1

Los resultados individuales de los cuestionarios realizados a empresas pueden consultarse en la empresa **XXX**, encontrándose los mismos en poder de **JESUS CANOVACA**. Las preguntas de cada uno de los cuestionarios han sido utilizadas como herramienta de trabajo para la realización del presente informe.

5. ANÁLISIS Y EVALUACIÓN

METODOLOGÍA UTILIZADA

La metodología utilizada para la realización del análisis y evaluación de los riesgos identificados es la matriz de probabilidad - impacto. Esta herramienta de análisis nos permite establecer prioridades en cuanto a los posibles riesgos en función tanto de la probabilidad de que ocurran como de las repercusiones que podrían tener sobre **EMPRESA XXX** en caso de que ocurrieran.

Una vez evaluadas las variables y obtenido un resultado en términos de **Probabilidad (P)** e **Impacto (I)**, se combinan entre sí dando como resultado el **Nivel de Riesgo Inherente** a la propia actividad de la compañía. **(Probabilidad x Impacto)**.

A su vez, el nivel de riesgo se divide en cinco niveles: **RIESGO MÍNIMO (azul), RIESGO LEVE (verde), MODERADO (amarillo), ALTO (naranja) y MUY ALTO (rojo)**, en función de las posibles combinaciones de probabilidad e impacto.

PERFIL DE RIESGO

Como punto de partida, **JESUS CANOVACA** ha determinado inicialmente un perfil de riesgo **MODERADO** para la empresa **EMPRESA XXX**, considerando como **ACEPTABLE** que el nivel de riesgo en todas las categorías se sitúe en el valor **LEVE**, en base a la siguiente configuración de niveles de la matriz que se muestra a continuación:

MUY ALTA					
ALTA					
MEDIA					
BAJA					
MUY BAJA					
P / I	MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO

NIVEL DE RIESGO
MINIMO
LEVE
MODERADO
ALTO
MUY ALTO

Con esta matriz de riesgos, se determina claramente qué riesgos suponen mayor amenaza para **EMPRESA XXX** y de esa manera nos permite gestionar eficientemente los recursos para prevenirlos.

[redacted]

MEDIDAS DE CONTROL

Una vez obtenido el mapa de Riesgos Inherente, se vuelve a valorar el grado de exposición de **EMPRESA XXX** a la materialización de los riesgos identificados, teniendo en cuenta las medidas de control ya existentes o que se hayan ido incorporando durante la detección de los riesgos.

Al igual que se hace con los riesgos identificados, para obtener una mayor aproximación a la realidad de la compañía, se evalúa cada medida de control para determinar su eficacia, y, por tanto, el nivel de mitigación del riesgo.

Las medidas de control que utiliza **EMPRESA XXX** para la mitigación de sus riesgos disponen de una serie de características en función de:

- El carácter **preventivo, detectivo o correctivo**:
  - Preventivos: anticipan eventos no deseados antes de que sucedan.
  - Detectivos: identifican los eventos en el momento en que se presentan.
  - Correctivos: aseguran que las acciones sean tomadas para minimizar el impacto generado.

[redacted]

RIESGO RESIDUAL

Una vez evaluadas las Medidas de Control, y aplicadas al Riesgo Inherente, se obtiene el Nivel de Riesgo Residual en el que se sitúa **EMPRESA XXX** en el momento del Análisis de Riesgos.
El nivel de riesgo residual se clasifica, al igual que el riesgo inherente, de acuerdo con los niveles establecidos: **RIESGO MÍNIMO (azul), RIESGO LEVE (verde), MODERADO (amarillo), ALTO (naranja) y MUY ALTO (rojo)** siguiendo la misma clasificación anterior.

PRIORIDAD DE ACCIONES

Cuando **EMPRESA XXX** detecta que su escenario de riesgo se sitúa en niveles **MODERADO (Vulnerabilidades Medias:** vulnerabilidad de compleja explotación, que puede permitir el bloqueo del sistema y robo de información), **ALTO** (**Vulnerabilidades Altas**: aquellas de fácil explotación que puede poner en riesgo el sistema y los datos que contiene) o **MUY ALTO** (**Vulnerabilidades Graves:** aquellas de muy fácil explotación que puede poner en riesgo el sistema y los datos que contiene) debe tomar las siguientes medidas encaminadas a reducir los riesgos en función de su clasificación:

NIVEL DE RIESGO	PRIORIDAD DE ACCIONES
LEVE	**BAJA:** No son necesarias acciones adicionales.
MODERADO	**MODERADA:** Se requiere de acciones a medio plazo por parte de los directores de los distintos departamentos de la Compañía. Requiere de seguimiento periódico convenido, mínimo dos veces al año.
ALTO	**ALTA:** Se requiere de acciones a corto plazo. Debe ponerse en conocimiento de la Dirección General para el análisis detenido de los riesgos y el estudio de implantación de nuevos controles previo análisis Costo_Beneficio de la inversión a realizar. Requiere de seguimiento periódico convenido, mínimo tres veces al año.
MUY ALTO	**MÁXIMA:** Se requiere de acciones inmediatas. Debe ponerse en conocimiento de la Dirección General para el análisis detenido de los riesgos y el estudio de implantación de nuevos controles previo análisis Costo_Beneficio de la inversión a realizar. Requiere de seguimiento continuo.

6. MATRIZ DE RIESGOS INHERENTE Y RESIDUAL

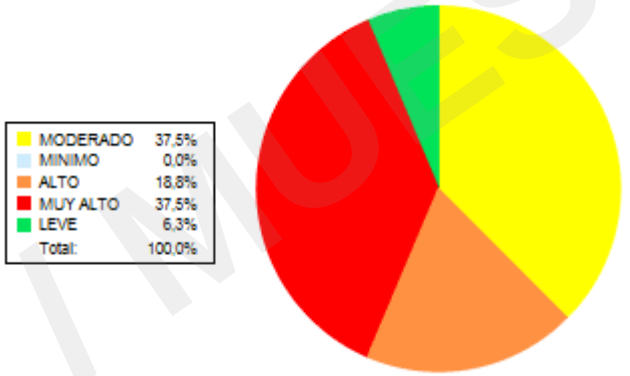
EVOLUCIÓN DE LA MATRIZ DE RIESGOS DE EMPRESA XXX

MATRIZ DE RIESGOS INHERENTES A LA ACTIVIDAD

Prob. / Impacto	MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
MUY ALTA	1		1	2	3
ALTA		1	1	1	1
MEDIA	1	2	2		
BAJA					
MUY BAJA					

Nº total de riesgos: 16

DISTRIBUCIÓN DEL RIESGO INHERENTE



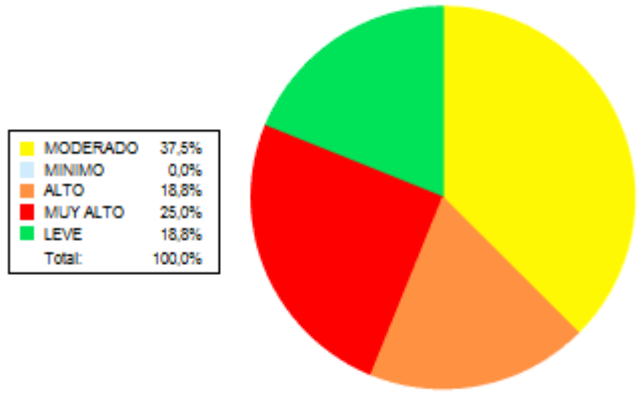
	Nº Riesgos	%Riesgos
Muy Alto	6	38
Alto	3	19
Moderado	6	38
Leve	1	6
Mínimo	0	0

MATRIZ DE RIESGOS RESIDUALES

Prob. / Impacto	MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
MUY ALTA	1		2	1	2
ALTA		1		1	1
MEDIA		2	2		
BAJA	2	1			
MUY BAJA					

Nº total de riesgos: 16

DISTRIBUCIÓN DEL RIESGO RESIDUAL



	Nº Riesgos	%Riesgos
Muy Alto	4	25
Alto	3	19
Moderado	6	38
Leve	3	19
Mínimo	0	0

7. MAPA DETALLADO DE RIESGOS Y CONTROLES

Como resultado del análisis realizado por el equipo de trabajo de **JESUS CANOVACA**, se detalla el resultado obtenido del Análisis de Riesgos de **EMPRESA XXX** en su situación actual, reflejando tanto el riesgo inherente a la propia actividad, como el riesgo residual tras la aplicación de los controles implementados en la empresa.

RIESGO	RIESGO INHERENTE	MEDIDA DE GESTIÓN IMPLANTADA	% RED.	RIESGO RESIDUAL
DEPENDENCIA TECNOLÓGICA	P: MUY ALTA, I: MUY ALTO			P: MUY ALTA, I: MUY ALTO
INCORRECTA SELECCIÓN Y FORMACIÓN Y COMPROMISO DEL PERSONAL	P: MUY ALTA, I: MUY ALTO			P: MUY ALTA, I: MUY ALTO
RESILIENCIA Y CONTINUIDAD DEL NEGOCIO	P: MUY ALTA, I: MUY ALTO			P: MUY ALTA, I: MUY ALTO
DAÑOS EN EL SISTEMA INFORMÁTICO O EN LOS ACTIVOS DE SU EMPRESA DERIVADOS DEL USO DE HARDWARE	P: MUY ALTA, I: ALTO	Configuración de un sistema de alertas. Recibir avisos y notificaciones sobre [illegible] actualizaciones y parches de seguridad.		P: MUY ALTA, I: ALTO
DAÑOS EN EL SISTEMA INFORMÁTICO Y/O LA RED DE LA EMPRESA DERIVADOS DEL USO DE SOFTWARE	P: ALTA, I: ALTO			P: ALTA, I: ALTO
INCIDENTES DE SEGURIDAD REACIONADOS CON EL ENTORNO DE LA EMPRESA	P: MUY ALTA, I: ALTO	PÓLIZA DE MULTIRRIESGO PYME. Cobertura daños materiales por incendio, daños [illegible]	24	P: MUY ALTA, I: MEDIO
INCORRECTO FUNCIONAMIENTO DE LA EXTERNALIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y CLOUD COMPUTING	P: MUY ALTA, I: MEDIO	Copias de seguridad en la nube	11	P: MUY ALTA, I: MEDIO
INCIDENTES/BRECHAS DE SEGURIDAD	P: MUY ALTA, I: MEDIO	[illegible] periódicas , protocolos de accesos no autorizados,	40	P: MEDIA, I: MEDIO
DAÑOS EN EL SISTEMA INFORMÁTICO O EN LOS ACTIVOS DE SU EMPRESA DERIVADOS DEL USO DE REDES DE TELECOMUNICACIONES	P: MUY ALTA, I: MEDIO	[illegible] e implantación en todos los equipos informáticos de la empresa, así como en todos los dispositivos [illegible] corporativas)	12	P: MEDIA, I: MEDIO
INCORRECTA GESTIÓN DE LAS CONTRASEÑAS	P: ALTA, I: BAJO			P: ALTA, I: BAJO
INCIDENTES RELACIONADOS CON EL ACCESO A LOS DATOS (COPIAS DE SEGURIDAD DE DATOS)	P: ALTA, I: MEDIO	Copias de Seguridad de los datos. (Actualizaciones periódicas , protocolos de [illegible] seguridad, cifrado para evitar accesos no autorizados, etc.)	40	P: MEDIA, I: BAJO
PÉRDIDA DE CONFIDENCIALIDAD DISPONIBILIDAD E INTEGRIDAD DE LOS DATOS PERSONALES	P: ALTA, I: MEDIO			P: MEDIA, I: BAJO
INCORRECTO FUNCIONAMIENTO DE SERVICIOS EXTERNALIZADOS	P: MUY ALTA, I: BAJO			P: MUY ALTA, I: MUY BAJO
DAÑOS EN EL SISTEMA INFORMÁTICO Y/O LA RED DE LA EMPRESA DERIVADOS DEL MAL USO DE DISPOSITIVOS MÓVILES	P: MEDIA, I: MEDIO	Actualización periódica de dispositivos móviles	11	P: BAJA, I: BAJO
		Implantación de sistemas [illegible] timalware. (Actualizado e implantación en todos los equipos informáticos de la empresa, así como en todos los dispositivos móviles que tengan posibilidad de acceso remoto a las cuentas corporativas)	12	

		DE GESTIÓN IMPLANTADA	% RED.	RIESGO RESIDUAL
ACCESOS INDEBIDOS	P: MEDIA, I: BAJO	Copias de Seguridad de los datos. (Actualizaciones periódicas , protocolos de acceso a estas copias de seguridad, cifrado para evitar accesos no autorizados, etc.)	40	P: BAJA, I: MUY BAJO
		Implantación de sistemas antimalware. (Actualizado e implantación en todos los equipos informáticos de la empresa así como en todos los dispositivos móviles que tengan posibilidad de acceso remoto a las cuentas corporativas)	12	
INCORRECTA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	P: MEDIA, I: MUY BAJO	Copias de Seguridad de los datos. (Actualizaciones periódicas , protocolos de acceso a estas copias de seguridad, cifrado para evitar accesos no autorizados, etc.)	40	P: BAJA, I: MUY BAJO

8. RECOMENDACIONES Y ACCIONES DE MEJORA

En base a las respuestas ofrecidas al cuestionario de identificación de medidas de gestión del ciberriesgo, se han identificado aquellas que **EMPRESA XXX** tiene implantadas en la actualidad.

JESUS CANOVACA ofrece a continuación una serie de acciones de mejora, orientadas a implantar medidas de gestión adicionales para aquellos riesgos que, por su exposición o impacto en caso de materialización, pueden suponer un perjuicio considerable para la empresa **EMPRESA XXX**.

Las siguientes tablas resumen el plan de acción a ejecutar, priorizando para el próximo ejercicio la implantación de aquellas medidas de gestión (tanto de control como de transferencia del riesgo) diseñadas para reducir aquellos riesgos con mayor nivel de riesgo residual detectados en el análisis. Concretamente, se recomienda implementar en el plazo de un año las medidas catalogadas con prioridad **MUY ALTA y ALTA**. Igualmente, en un segundo ejercicio, se propone de manera óptima la implementación de las medidas incluidas con prioridad **MODERADA**.

La revisión de la ejecución de este plan de acción podría ser realizada mediante [illegible] que **EMPRESA XXX** contrate a **JESUS CANOVACA**, cuyo alcance quedaría fuera de este documento y debería ser definido en un nuevo documento.

MEDIDA DE GESTIÓN A IMPLANTAR	TIPO	PRIORIDAD
PÓLIZA DE CIBERRIESGO PYME. Cobertura: Daños Propios (restauración de la información afectada y la recuperación de los sistemas dañados, con el objetivo de volver a la situación anterior al ciberataque)	PÓLIZA	MUY ALTA
PÓLIZA DE CIBERRIESGO PYME. Cobertura: Responsabilidad Civil (garantiza las posibles reclamaciones de terceros (clientes, proveedores o trabajadores), por cualquier tipo de incumplimiento, debido a fallos en la seguridad, vulneración de datos o daños morales en internet.)	PÓLIZA	MUY ALTA
PÓLIZA DE D&O (Consejeros y directivos). Coberturas: procedimientos civiles y penales, gastos de defensa por reclamaciones en seguridad y salud laboral, incumplimiento normativo.	PÓLIZA	MUY ALTA
Actualización periódica de equipos y aplicaciones	CONTROL	MUY ALTA
Cláusulas contractuales y acuerdos de confidencialidad. (Reflejo en los contratos laborales de los empleados los aspectos más importantes en materia de ciberseguridad y confidencialidad)	CONTROL	MUY ALTA
Formación a empleados en seguridad de la información.	CONTROL	MUY ALTA
Gestión de los permisos y niveles de acceso entre los empleados y responsables de la empresa.	CONTROL	MUY ALTA
Guía de buenas prácticas de movilidad o teletrabajo	CONTROL	MUY ALTA
Herramientas de diagnóstico y actualización para detectar software no actualizado en tus equipos.	CONTROL	MUY ALTA
Plan de Contingencia y Continuidad de Negocio -Alcance -Responsabilidades -Evaluación de impacto -Capacidad -Estrategia de contingencia	CONTROL	MUY ALTA
Política de seguridad en el puesto de trabajo	CONTROL	MUY ALTA
Protocolo de seguridad informática. (Normas y procedimientos y manual de buenas prácticas para los empleados)	CONTROL	MUY ALTA
Auditoría de software instalado	CONTROL	ALTA
Cláusulas contractuales y acuerdos de confidencialidad. (Reflejo en los contratos con terceros los aspectos más importantes en materia de ciberseguridad y confidencialidad)	CONTROL	ALTA
Código disciplinario en materia de usos no autorizados	CONTROL	ALTA
Normativa de destrucción de documentos y soportes	CONTROL	ALTA
Normativa de uso de software legal o política de aplicaciones permitidas	CONTROL	ALTA
Política de seguridad del proveedor.	CONTROL	ALTA
Proceso de borrado de la información en la nube.	CONTROL	ALTA
Sistema de alimentación ininterrumpida (SAI). Dispositivo eléctrico que proporciona energía de emergencia a un equipo	CONTROL	ALTA
Monitorización y registro de la actividad	CONTROL	MODERADA
Normativa o política de uso de dispositivos móviles.	CONTROL	MODERADA
Política de contraseñas	CONTROL	MODERADA
Restricción de acceso (mediante bloqueo o contraseña) a los equipos por parte de personal ajeno a la organización.	CONTROL	MODERADA

A continuación, se detallan las medidas de gestión a implantar por orden de prioridad, identificando qué riesgos se verán mitigados por cada una de ellas.
La tabla muestra los registros ordenados por orden de prioridad de implantación de las medidas.

A modo de ejemplo práctico, primero se muestran las medidas con prioridad **MUY ALTA**, es decir, aquellas que mitigan riesgos que **EMPRESA XXX** tiene en un nivel residual **MUY ALTO**. Así mismo y a continuación se muestran aquellas medidas con prioridad **ALTA**, es decir, aquellas que mitigan riesgos que **EMPRESA XXX** tiene en un nivel residual **ALTO** y así con el resto de medidas propuestas, con niveles de prioridad de implantación decrecientes.

PRIORIDAD	MEDIDA DE GESTIÓN A IMPLANTAR	RIESGOS MITIGADOS	R.R.
MUY ALTA	Actualización periódica de equipos y aplicaciones	DAÑOS EN EL SISTEMA INFORMATICO O EN LOS ACTIVOS DE SU EMPRESA DERIVADOS DEL USO DE HARDWARE.	
		DAÑOS EN EL SISTEMA INFORMÁTICO Y/O LA RED DE LA EMPRESA DERIVADOS DEL USO DE SOFTWARE	
	Cláusulas contractuales y acuerdos de confidencialidad. (Reflejo en los contratos laborales de los empleados los aspectos más importantes en materia de ciberseguridad y confidencialidad)	INCORRECTA SELECCIÓN Y FORMACIÓN Y COMPROMISO DEL PERSONAL	
	Formación a empleados en seguridad de la información		
		DAÑOS EN EL SISTEMA INFORMÁTICO Y/O LA RED DE LA EMPRESA DERIVADOS DEL USO DE SOFTWARE	
		DAÑOS EN EL SISTEMA INFORMATICO O EN LOS ACTIVOS DE SU EMPRESA DERIVADOS DEL USO DE REDES DE TELECOMUNICACIÓNES.	
		INCIDENCIAS DE SEGURIDAD	
		INCORRECTA GESTIÓN DE CONTRASEÑAS	
		CONFIDENCIALIDAD DISPONIBILIDAD E INTEGRIDAD DE LOS DATOS PERSONALES	
		DAÑOS EN EL SISTEMA INFORMATICO Y/O LA RED DE LA EMPRESA DERIVADOS DEL MAL USO DE DISPOSITVOS MÓVILES	
		ACCESOS INDEBIDOS	
	Gestión de los permisos y niveles de acceso entre los empleados y responsables de la empresa	INCORRECTA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	
		DEPENDENCIA TECNOLÓGICA	
		ACCESOS INDEBIDOS	
		INCORRECTA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	
	Cláusulas contractuales de movilidad o teletrabajo	DEPENDENCIA TECNOLÓGICA	
	Herramientas de gestión y actualización para detectar software no actualizado en los equipos.	DAÑOS EN EL SISTEMA INFORMATICO O EN LOS ACTIVOS DE SU EMPRESA DERIVADOS DEL USO DE HARDWARE.	

PRIORIDAD	MEDIDA DE GESTIÓN A IMPLANTAR	RIESGOS MITIGADOS	R.R.
[redacted]			

PRIORIDAD	MEDIDA DE GESTIÓN A IMPLANTAR	RIESGOS MITIGADOS	R.R.
MEDIA	Protocolo de seguridad informática. (Normas y procedimientos y manual de buenas practicas para los empleados)	INCORRECTA SELECCIÓN Y FORMACIÓN Y COMPROMISO DEL PERSONAL	
		DAÑOS EN EL SISTEMA INFORMATICO O EN LOS ACTIVOS DE SU EMPRESA DERIVADOS DEL USO DE HARDWARE.	
		RESILIENCIA Y CONTINUIDAD DEL NEGOCIO	
		INCIDENTES DE SEGURIDAD REACIONADOS CON EL ENTORNO DE LA EMPRESA	
		INCORRECTO FUNCIONAMIENTO DE LA EXTERNALIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y CLOUD COMPUTING	
		DAÑOS EN EL SISTEMA INFORMATICO O EN LOS ACTIVOS DE SU EMPRESA DERIVADOS DEL USO DE REDES DE TELECOMUNICACIÓNES.	
		ACCIDENTES Y BRECHAS DE SEGURIDAD	
		INCORRECTA GESTIÓN DE CONTRASEÑAS	
		[illegible] CIONADOS CON EL ACCESO A LOS DATOS (COPIAS DE SEGURIDAD DE DATOS)	
		[illegible] CIALIDAD DISPONIBILIDAD E INTEGRIDAD DE LOS DATOS PERSONALES	
		[illegible] ÑOS EN EL SISTEMA INFORMATICO Y/O LA RED DE LA EMPRESA DERIVADOS DEL MAL USO DE DISPOSITVOS MÓVILES	
		ACCESOS INDEBIDOS [illegible]	
		INCORRECTA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	
ALTA	Auditoria de software instalado	DAÑOS EN EL SISTEMA INFORMÁTICO Y/O LA RED DE LA EMPRESA DERIVADOS DEL USO DE SOFTWARE	
	Cláusulas contractuales y acuerdos de confidencialidad. (Incluir en los contratos con terceros los aspectos mas importantes de la LOPD, seguridad y confidencialidad)	INCORRECTO FUNCIONAMIENTO DE LA EXTERNALIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y CLOUD COMPUTING	
		INCORRECTO FUNCIONAMIENTO DE SERVICIOS EXTERNALIZADOS	
	Cumplimiento de la [illegible] de uso de software	DAÑOS EN EL SISTEMA INFORMÁTICO Y/O LA RED DE LA EMPRESA DERIVADOS DEL USO DE SOFTWARE	
	[illegible] alternativa de destrucción de documentos y soportes	INCIDENTES DE SEGURIDAD REACIONADOS CON EL ENTORNO DE LA EMPRESA	

PRIORIDAD	MEDIDA DE GESTIÓN A IMPLANTAR	RIESGOS MITIGADOS	R.R.
ALTA	Normativa de destrucción de documentos y soportes	INCIDENTES RELACIONADOS CON EL ACCESO A LOS DATOS (COPIAS DE SEGURIDAD DE DATOS)	
		PÉRDIDA DE CONFIDENCIALIDAD DISPONIBILIDAD E INTEGRIDAD DE LOS DATOS PERSONALES	
		INCORRECTA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	
	Normativa de uso de software legal o política de aplicaciones permitidas	DAÑOS EN EL SISTEMA INFORMÁTICO Y/O LA RED DE LA EMPRESA DERIVADOS DEL USO DE SOFTWARE	
	Política de seguridad de los proveedores	INCORRECTO FUNCIONAMIENTO DE LA EXTERNALIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y CLOUD COMPUTING	
		INCORRECTO FUNCIONAMIENTO DE SERVICIOS EXTERNALIZADOS	
	Proceso de borrado de la información en la nube	INCORRECTO FUNCIONAMIENTO DE LA EXTERNALIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y CLOUD COMPUTING	
	Sistema de alimentación ininterrumpida (SAI). Dispositivo eléctrico que proporciona energía	INCIDENTES DE SEGURIDAD RELACIONADOS CON EL ENTORNO DE LA EMPRESA	
MEDIA	Monitorización y registro	[illegible] INFORMATICO O EN LOS ACTIVOS DE SU EMPRESA [illegible] EL USO DE REDES DE TELECOMUNICACIÓNES.	
	Normativa de [illegible]		
		DAÑOS EN EL SISTEMA INFORMÁTICO Y/O LA RED DE LA EMPRESA DERIVADOS DEL MAL USO DE DISPOSITVOS MÓVILES	
	Política de contraseñas	INCORRECTA GESTIÓN DE CONTRASEÑAS	
	Restricción de acceso (mediante bloqueo o contraseñas) a lugares específicos por parte de personal ajeno a la organización	INCORRECTO FUNCIONAMIENTO DE SERVICIOS EXTERNALIZADOS	

9. MATRIZ DE RIESGO RESIDUAL ANTES Y TRAS LA EJECUCIÓN DEL PLAN

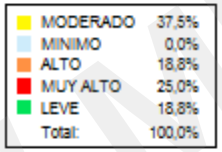
EVOLUCIÓN DE LA MATRIZ DE RIESGOS DE EMPRESA XXX

MATRIZ DE RIESGO RESIDUAL ANTES DE EJECUTAR EL PLAN

Prob. / Impacto	MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
MUY ALTA	1		2	1	2
ALTA		1		1	1
MEDIA		2	2		
BAJA	2	1			
MUY BAJA					

Nº total de riesgos: 16

DISTRIBUCIÓN DEL RIESGO



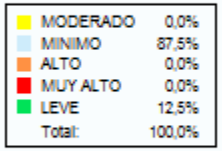
	Nº Riesgos	%Riesgos
Muy Alto	4	25
Alto	3	19
Moderado	6	38
Leve	3	19
Mínimo	0	0

MATRIZ DE RIESGO RESIDUAL TRAS EJECUTAR EL PLAN

Prob. / Impacto	MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
MUY ALTA					
ALTA					
MEDIA	1				
BAJA	1				
MUY BAJA	14				

Nº total de riesgos: 16

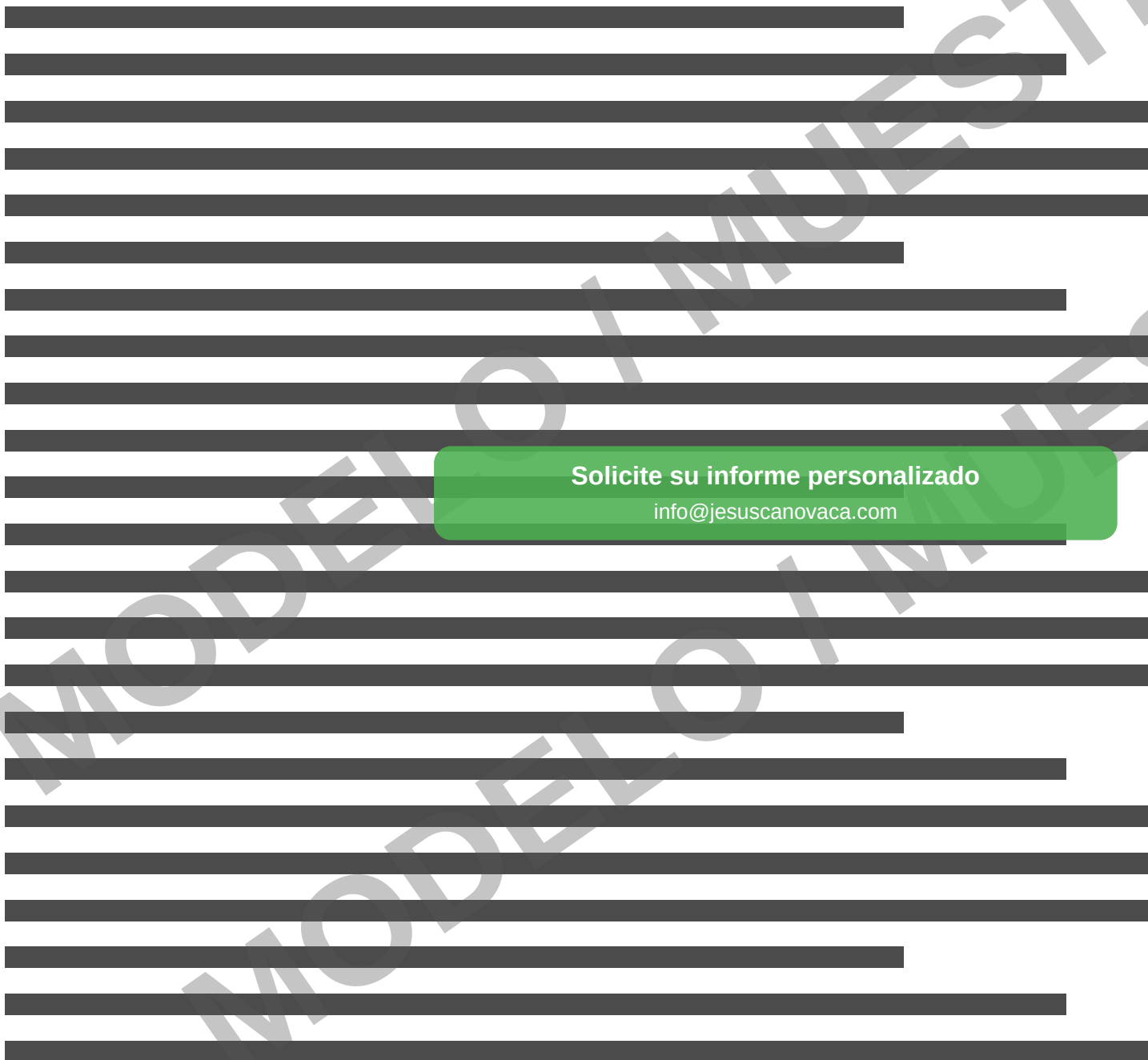
DISTRIBUCIÓN DEL RIESGO



	Nº Riesgos	%Riesgos
Muy Alto	0	0
Alto	0	0
Moderado	0	0
Leve	2	13
Mínimo	14	88

10. MAPA DE RIESGOS Y MEDIDAS TRAS LA EJECUCIÓN DEL PLAN

Por último, se detalla ahora el siguiente mapa de riesgos inherente y residual optimizado tras la ejecución del plan de acción propuesto, en base a las recomendaciones incluidas en él, resaltando en color AZUL CELESTE aquellas medidas propuestas por **JESUS CANOVACA** y sin resaltar aquellas otras que **EMPRESA XXX** ya tiene implantadas en la actualidad:



RIESGO	RIESGO INHERENTE	MEDIDA DE GESTIÓN IMPLANTADA	% RED.	RIESGO RESIDUAL
RESILIENCIA Y CONTINUIDAD DEL NEGOCIO	P: ALTA, I: MUY ALTO	[redacted]	80	P: MEDIA, I: MUY BAJO
		POLIZA DE CIBERRIESGO PYME.	80	
		[redacted]	80	
		[redacted]	80	
INCIDENTES DE SEGURIDAD RESPONDIDOS DE UN ENTORNO DE LA EMPRESA	[redacted]	[redacted]	80	[redacted] Y BAJO
		[redacted]	30	
		[redacted]	25	
DEPENDENCIA TECNOLÓGICA	P: MUY ALTA, I: MUY [redacted]	Gestión de los permisos y niveles de acceso entre los empleados y responsables de la empresa	40	P: MUY BAJA, I: MUY BAJO
		Guía de buenas prácticas de movilidad o teletrabajo	30	
		Plan de Contingencia y Continuidad de Negocio -Alcance -Responsabilidades -Evaluación de Impacto -Criticidad -Estrategia de contingencia	20	

INCORRECTA SELECCIÓN Y FORMACIÓN Y COMPROMISO DEL PERSONAL	P: MUY ALTA, I: MUY ALTO	PÓLIZA DE CIBERRIESGO PYME. Cobertura: Responsabilidad Civil (garantiza las posibles reclamaciones de terceros (clientes, proveedores o trabajadores), por cualquier tipo de incumplimiento, debido a fallos en la seguridad, vulneración de datos o daños morales en internet)	80	P: MUY BAJA, I: MUY BAJO
		Cláusulas contractuales y acuerdos de confidencialidad. (Reflejo en los [illegible] de ciberseguridad y confidencialidad)	30	
		[illegible] empleados en seguridad de la información.	30	
		[illegible] de seguridad en el puesto de trabajo.	30	
		Protocolo de seguridad informática. (Normas y procedimientos y manual de buenas prácticas para los empleados)	30	
ACCESOS INDEBIDOS	P: MEDIA, I: BAJO	Copias de Seguridad de los datos. (Actualizaciones periódicas , protocolos de acceso a estas copias de seguridad, cifrado para evitar accesos no autorizados, etc)	40	P: MUY BAJA, I: MUY BAJO
		[illegible] de implantación en todos los dispositivos móviles que tengan [illegible] acceso remoto a las cuentas corporativas)	12	
		Formación a empleados en seguridad de la información.	30	
		Gestión de los permisos y niveles de acceso entre los empleados y [illegible]	40	
		Protocolo de seguridad informática. (Normas y procedimientos y manual de buenas prácticas para los empleados)	30	
INCORRECTA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	P: MEDIA, I: MUY BAJO	Copias de Seguridad de los datos. (Actualizaciones periódicas , protocolos de acceso a estas copias de seguridad, cifrado para evitar accesos no autorizados, etc)	40	P: MUY BAJA, I: MUY BAJO
		PÓLIZA DE CIBERRIESGO PYME. Cobertura: Responsabilidad Civil (garantiza las posibles reclamaciones de terceros (clientes, proveedores o trabajadores), por cualquier tipo de incumplimiento, debido a fallos en la seguridad, vulneración de datos o daños morales en internet)	80	
		[illegible] recuperación de los sistemas dañados, con el objetivo de volver a la situación anterior al [illegible]		
		PÓLIZA DE CIBERRIESGO PYME. Cobertura: Responsabilidad Civil (garantiza las posibles reclamaciones de terceros (clientes, proveedores o trabajadores), por cualquier tipo de incumplimiento, debido a fallos en la seguridad, vulneración de datos o daños morales en internet)	80	

[redacted]

INCORRECTA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	P: MEDIA, I: MUY BAJO	Formación a empleados en seguridad de la información.	30	P: MUY BAJA, I: MUY BAJO
		Gestión de los permisos y niveles de acceso entre los empleados responsables de la empresa.	40	
		Normativa de [illegible] documentos y soportes	[illegible]	
		Protocolo de seguridad informática. (Normas y procedimientos y manual de buenas prácticas para los empleados)	[illegible]	
INCIDENTES/BRECHAS DE SEGURIDAD	P: MUY ALTA, I: MUY ALTO	Copias de seguridad de los datos. (Actualizaciones periódicas , protocolos de acceso a estas copias de seguridad, cifrado para evitar accesos no autorizados, etc)	40	P: MUY BAJA, I: MUY BAJO
		POLIZA DE CIBERRIESGO PYME: Cobertura: Daños Propios (restauración de la información afectada y la recuperación de los sistemas dañados para volver a la situación anterior al ciberataque)	80	
		[illegible] reclamaciones de cualquier tipo de [illegible] de datos o daños morales en internet	80	
		Formación a empleados en seguridad de la información.	30	
		Protocolo de seguridad informática. (Normas y procedimientos y manual de buenas prácticas para los empleados)	[illegible]	
INCIDENTES/BRECHAS DE SEGURIDAD (COPIAS DE SEGURIDAD DE DATOS)	P: MUY ALTA, I: MUY ALTO	Copias de seguridad de los datos. (Actualizaciones periódicas , protocolos de acceso a estas copias de seguridad, cifrado para evitar accesos no autorizados, etc)	40	P: MUY BAJA, I: MUY BAJO
		[illegible] portes	30	
		Protocolo de seguridad informática. (Normas y procedimientos y manual de buenas prácticas para los empleados)	30	
INCORRECTA GESTIÓN DE CONTRASEÑAS	P: MEDIA, I: MUY BAJO	[illegible] empleados en seguridad de la información.	[illegible]	P: MUY BAJA, I: MUY BAJO
		Política de contraseñas	40	
		Protocolo de seguridad informática. (Normas y procedimientos y manual de buenas prácticas para los empleados)	30	

PÉRDIDA DE CONFIDENCIALIDAD DISPONIBILIDAD E INTEGRIDAD DE LOS DATOS PERSONALES	P: MEDIA, I: BAJO	PÓLIZA DE CIBERRIESGO PYME	80	P: MUY BAJA, I: MUY BAJO
		POLIZA DE D&O (Consejeros y directivos).	80	
		Formación a empleados en seguridad de la información.	30	
		Política de destrucción de documentos y soportes	30	
		Protocolo de seguridad informática. (Normas y procedimientos y manual de buenas prácticas para los empleados)	30	
DAÑOS EN EL SISTEMA INFORMÁTICO O EN LOS ACTIVOS DE SU EMPRESA DERIVADOS DEL USO DE HARDWARE	P: MUY ALTA, I: ALTO	Configuración de un sistema de alertas: Recibir avisos y notificaciones sobre	9	P: MUY BAJA, I: MUY BAJO
			80	
			35	
		Herramientas de diagnóstico y actualización para detectar software no actualizado en tus equipos.	0	
		Protocolo de seguridad informática. (Normas y procedimientos y manual de buenas prácticas para los empleados)	0	
DAÑOS EN EL SISTEMA INFORMÁTICO Y/O LA RED DE LA EMPRESA DERIVADOS DEL USO DE SOFTWARE	P: MUY ALTA, I: ALTO	Actualización periódica de equipos y aplicaciones	35	P: MUY BAJA, I: MUY BAJO
		Auditoria de software instalado	25	
		Código disciplinario en materia de uso no autorizado de software.	30	
		Formación a empleados en seguridad de la información.	30	
		Normativa de uso de software legal o política de aplicaciones permitidas	30	

DAÑOS EN EL SISTEMA INFORMATICO O EN LOS ACTIVOS DE SU EMPRESA DERIVADOS DEL USO DE REDES DE TELECOMUNICACIÓNES.	P: MEDIA, I: MEDIO	Implantación de sistemas antimalware. (Actualizado e implantación en todos los equipos informáticos de la empresa, así como en todos los dispositivos móviles que tengan posibilidad de acceso remoto a las cuentas corporativas)	12	P: MUY BAJA, I: MUY BAJO
		PÓLIZA DE CIBERSEGURIDAD. Cobertura: Daños Propios (restauración de la información afectada y la reconstrucción de los sistemas afectados, con el objetivo de dejarlos tal y como estaban antes del ciberataque)	30	
		Formación a empleados en seguridad de la información.	30	
		Autorización y registro de la actividad.	40	
		Normativa o política de uso de dispositivos móviles.	30	
		Protocolo de seguridad informática. (Normas y procedimientos y manual de buenas prácticas para los empleados)	30	
DAÑOS EN EL SISTEMA INFORMATICO Y/O LA RED DE LA EMPRESA DERIVADOS DEL MAL USO DE DISPOSITIVOS MOVILES	P: MUY BAJA, I: MUY BAJO		11	P: MUY BAJA, I: MUY BAJO
		Implantación de sistemas antimalware. (Actualizado e implantación en todos los equipos informáticos de la empresa, así como en todos los dispositivos móviles que tengan posibilidad de acceso remoto a las cuentas corporativas)	12	
		Formación a empleados en seguridad de la información.	30	
		Normativa o política de uso de dispositivos móviles.	30	
		Protocolo de seguridad informática. (Normas y procedimientos y manual de buenas prácticas para los empleados)	30	
INCORRECTO FUNCIONAMIENTO DE LA EXTERNALIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y CLOUD COMPUTING	P: MUY BAJA, I: MEDIO	Copias de seguridad en la nube.	11	P: MUY BAJA, I: MUY BAJO
		Cláusulas contractuales y acuerdos de confidencialidad. (Reflejo en los contratos con terceros los aspectos más importantes en materia de ciberseguridad y confidencialidad)	30	
		Política de seguridad del proveedor.	30	
		Proceso de borrado de la información en la nube.	30	

INCORRECTO FUNCIONAMIENTO DE LA EXTERNALIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y CLOUD COMPUTING	P: MUY ALTA, I: MEDIO	Protocolo de seguridad informática. (Normas, procedimientos y manual de buenas prácticas para los empleados)	30	P: MUY BAJA, I: MUY BAJO
INCORRECTO FUNCIONAMIENTO DE SERVICIOS EXTERNALIZADOS	P: MUY ALTA, I: MUY BAJO	Cláusulas contractuales y acuerdos de confidencialidad. (Reflejo en los contratos con proveedores de los aspectos más importantes en materia de ciberseguridad y confidencialidad)	30	P: MUY BAJA, I: MUY BAJO
		Control de acceso físico (mediante bloqueo o contraseñas) a lugares específicos mediante de personal ajeno a la organización.	30	

MEDIDAS DE GESTIÓN RECOMENDADAS

11. PÓLIZAS CONTRATADAS, PROPUESTAS Y GARANTÍAS MEJORABLES

PÓLIZA DE MULTIRRIESGO DAÑOS MATERIALES PYME

Garantía Opcional: Daños materiales que incluya daños físicos a los equipos.

PÓLIZA DE RESPONSABILIDAD CIVIL DE CONSEJEROS Y DIRECTIVOS

Garantía Básica: procedimientos civiles y penales, gastos de defensa por reclamaciones en seguridad y salud laboral, incumplimiento normativo.

PÓLIZA DE CIBERRIESGO PYME

Garantía Básica: Responsabilidad Civil (garantiza las posibles reclamaciones de terceros (clientes, proveedores o trabajadores), por cualquier tipo de incumplimiento, debido a fallos en la seguridad, vulneración de datos o daños morales en internet.)

Garantía Opcional: Daños Propios (restauración de la información afectada y la recuperación de los sistemas dañados, con el objetivo de volver a la situación anterior al ciberataque)

PÓLIZAS / GARANTÍAS PROPUESTAS	GARANTÍAS CONTRATADAS MEJORABLES

12. RESUMEN FINAL Y CONCLUSIONES

Nº RIESGOS IDENTIFICADOS	NIVEL RIESGO INHERENTE PROMEDIO	Nº MEDIDAS DE CONTROL (REDUCCIÓN RIESGO)	Nº MEDIDAS DE TRANSFERENCIA DEL RIESGO	NIVEL RIESGO RESIDUAL PROMEDIO
16	P: ALTA, I: MEDIO	5	1	P: MEDIA, I: BAJO

La identificación y análisis de los supuestos de riesgo o amenazas que pudieran afectar a **EMPRESA XXX** y cuyo resultado se traslada en el presente Informe, ha permitido obtener un mapa de riesgos con el objetivo de determinar el mejor modo de priorizar y gestionar dichos riesgos.

El Informe de Análisis de Riesgos supone el primer paso para la implantación de un sistema de Gestión de Riesgos en la Compañía que permita crear la estructura de **prevención y detección de riesgos acorde con sus características y recursos**.
El principal objetivo es mejorar los procedimientos y controles establecidos actualmente en la compañía con el fin de dar cobertura a las conductas de riesgo logrando así un nivel razonable de seguridad.

El diseño de este mapa de riesgos no es una tarea puntual, sino un proceso continuo y retroalimentado en el que deben integrarse los responsables de la compañía por lo que, concluida esta primera fase, es necesario analizar los resultados obtenidos con el objeto de identificar posibilidades de mejoras.

A ese respecto, **JESUS CANOVACA,** comprometida con el buen funcionamiento y la reducción de efectos adversos que los riesgos puedan suponer para **EMPRESA XXX**, realiza un análisis de todos aquellos riesgos existentes y mejorables susceptibles de ser transferidos a través de PÓLIZAS DE SEGUROS planteando los mejores escenarios en cuanto a cobertura y coste de la medida de control.

13. ANEXOS

a. BUENAS PRÁCTICAS EN GESTIÓN DE CIBERRIESGOS

COMPRENDE Y GESTIONA TUS RIESGOS

- Decide quién o quiénes serán los responsables de gestionar los riesgos de seguridad TI (Tecnología de la Información) en tu empresa.
- Elige qué nivel de riesgo estás dispuesto a aceptar.
- Elabora una Política de Seguridad que describa, paso a paso, qué estás dispuesto a hacer para gestionar los riesgos. Revísala al menos cada año para asegurarte que se ajusta a tus riesgos reales.
- Distribuye las responsabilidades de seguridad TI entre tus colaboradores y asegúrate que comprenden y asimilan su importancia.

ACTUALIZA TU SOFTWARE (CONFIGURACIONES SEGURAS)

- Haz un inventario con todos tus activos de tecnologías de la información (instalaciones, equipos, programas, software, etc.) para ser consciente de lo que tienes y de su valor.
- Actualiza sistemas operativos, softwares, firewares, etc. con parches y actualizaciones periódicas. Puedes activar la opción de «actualización automática» durante la instalación de muchos paquetes de software.
- Asegúrate de que tienes licencias de todo el software instalado.
- Revisa, periódicamente, las debilidades de tus sistemas mediante un análisis de vulnerabilidades. Al menos hazlo una vez al año o cuando realices algún cambio importante de hardware o software.

PROTEGE TU RED

- Protege tu red contra ataques externos.
- Comprueba si el dispositivo que conecta tu organización a Internet –el router que te ha proporcionado el proveedor de Internet– incluye Firewall, que te permitirá controlar las conexiones de red del acceso a Internet. Si no es así, instala uno que incluya esta funcionalidad para tus equipos.
- Sigue las instrucciones del fabricante para mantenerlo bien configurado y actualizado. Permanece alerta a los mensajes que te vaya indicando.
- Consulta con un experto si sospechas que tu red ha sido comprometida o si observas una actividad poco habitual.
- Restringe el acceso a Internet.

INSTALA DEFENSAS CONTRA MALWARES

- Utiliza en todos los equipos de la empresa un antimalware (algo más que un antivirus), o un paquete de seguridad con esta funcionalidad. Evita los gratuitos.
- Utiliza todas las prestaciones (antivirus, antispyware) que te ofrezca el paquete, aunque para ello haya que cambiar algunos hábitos. Asegúrate de que el escaneado se realiza al menos cada día y configura la herramienta para que se actualice automáticamente.
- Permite exclusivamente el uso de CD, DVD, USB, tarjetas SD o cualquier tipo de memoria flash que proporcione tu administrador de sistemas. Vigila su uso, dónde están, quién los tiene y qué contienen.
- Asegúrate que permitan cifrado y de que son escaneados para detectar malware cada vez que se usen. Muchos paquetes antimalware tienen la opción de analizar los dispositivos y medios extraíbles.

GESTIONA EL ACCESO A TUS SISTEMAS (PRIVILEGIOS DE USUARIO)

[redacted]

ENSEÑA BUENAS PRÁCTICAS (SENSIBILIZACIÓN Y FORMACIÓN DE USUARIOS)

- Asegúrate que todos los colaboradores conocen y aplican la Política de Seguridad definida y de que se insiste en su importancia en el protocolo de admisión de nuevos empleados.
- Incluye el cumplimiento de la Política como una clausula en los contratos.
- Recuerda, periódicamente, a los colaboradores, las buenas prácticas de seguridad, especialmente cuando cambia la Política o los riesgos.
- Si tu empresa utiliza Redes Sociales asegúrate de que los colaboradores están al tanto de cómo se deben comportar en las mismas cuando representan a la empresa y de que existen documentos que no se pueden compartir (sensibles o sujetos a propiedad intelectual).

CONTROLA LOS DISPOSITIVOS MÓVILES DE LOS COLABORADORES

[redacted]

b. RECOMENDACIONES DE SEGURIDAD PARA EMPLEADOS

Puesto de Trabajo

Mantén tu escritorio limpio de papeles que contengan información sensible. Bloquea la sesión de tu equipo cuando no estés en tu escritorio.

Dispositivos

No modifiques la configuración de los dispositivos de tu empresa. No instales aplicaciones no autorizadas. No conectes dispositivos USB no confiables.

Uso de Equipos No Corporativos

No manejes información corporativa en equipos públicos. Si accedes al correo corporativo desde tu equipo personal no descargues ficheros al equipo

Fugas de Información

No facilites información sensible si no estás seguro de quién es el receptor de la misma. Destruye la información sensible en formato papel. No la tires al basurero. No mantengas conversaciones confidenciales en lugares donde pueden ser oídas por terceros.

Gestión de Credenciales

No compartas tus credenciales de acceso (usuario y contraseña).No utilices tus credenciales de acceso corporativas en aplicaciones de uso personal.No dejes tus credenciales en lugares visibles.

Navegación

Evita acceder a páginas web no confiables. No pinches en enlaces (links) sospechosos.

Protección de la información

Realiza copias de seguridad de aquella información sensible que solo esté alojada en tus dispositivos.

Viaje seguro

Procura no transportar información confidencial