Concejo Municipal De Yumbo	INFORME DE GESTION Y CERTIFICADO DE SUPERVISOR	FO-GJ-11 Versión: 4 Fecha: 20-2-2020 Página 1 de 3

1. A SEGUIMIENTO ADMINISTRATIVO

2023-12-28 17:52 Us VENTANILLA5
DESTINO: CONCEJO MUNICIPAL DE YUMBO
REM/DES : JULIO POTOSI
ASUNTO: INFORME DE GESTION MES DE DICI
TRD:100-5-1 --CONTRATACIONES /CONTRATACION DI
/Informe De GestiÃ
202301000015906

IDENTIFICACIÓN DEL CONTRATO:	100.0501.019
CONTRATISTA:	JULIO POTOSI GUAMPE
OBJETO CONTRACTUAL:	PRESTAR POR SUS PROPIOS MEDIOS Y AUTONOMIA ADMINISTRATIVA LOS SERVICIOS PROFESIONALES DE APOYO A LAS GESTION EM EL CONCEJO MUNICIPAL
VALOR DEL CONTRATO:	$ 38.500.000
PLAZO DE EJECUCIÓN:	10 MESES
FECHA DE INICIO:	A PARTIR DE LA FIRMA DEL ACTA DE INICIO HASTA EL 26 DE DICIEMBRE DE 2023.
FECHA DE TERMINACION:	26 DICIEMBRE 2023
FORMA DE PAGO:	Para todos los efectos legales y fiscales se estima el valor del contrato de Prestación de Servicios Profesionales de Apoyo a la Gestión en la suma de TREINTA Y OCHO MILLONES QUINIENTOS MIL PESOS M/CTE ($38.500.000). EL CONTRATANTE cancelará el valor del contrato dentro de los cinco (5) primeros días de cada mes vencido previo recibo a satisfacción, de la siguiente manera: Once (11) pagos mensuales por valor de TRES MILLONES QUINIENTOS MIL PESOS M/CTE (S3.500.000) incluidos todos los costos derivados de la ejecución del contrato, correspondiente a los meses de febrero. marzo, abril, mayo. junio, julio, agosto, septiembre, octubre, noviembre y diciembre.
NOMBRE Y CARGO SUPERVISOR (ES) DEL CONTRATO:	MARISOL HERNANDEZ SANCHEZ
PERIODO DE SUPERVISIÓN:	DICIEMBRE

2. SEGUIMIENTO TÉCNICO

Actividades Contratadas	Actividades Ejecutadas	Registro o Evidencia de la Actividad	Ubicación Física del registro o evidencia
1. Brindar apoyo en la elaboración del plan de tratamiento de datos	Se proyecto documento relacionado con el Plan de tratamiento de satos personales para dar	PLAN DE RATAMIENTOS DE DATOS PERSONALES - CONCEJO	Proceso de bienes y servicios del Concejo Municipal de Yumbo

	cumplimientos a la ley 1581 de 2012	MUNICIPAL DE YUMBO	
1. Brindar apoyo en la revisión, ajuste y actualización del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y al Plan de Seguridad y Privacidad de la Información	Se realizo actualización de los plan de seguridad y privacidad, Plan de tratamiento de riesgos de seguridad de la información	1. Documento PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACION	Proceso de bienes y servicios del Concejo Municipal de Yumbo
2. Realizar Backus para salvaguardar la información de los aplicativos ASCII, Orfeo y la nube	Se realizaron copias de seguridad a los aplicativos ASCII, Orfeo y archivos en la nueve Nexcloud	Se realiza copias de seguridad de la base de datos Orfeo, ASCII e información del servidor principal de los activos digitales de información	Proceso de bienes y servicios del Concejo Municipal de Yumbo
3. Apoyo en la implementación del software de mesa de ayuda	Se realizo informe relacionado con la implementación de software GLPI para proceso Mesa de Ayuda	INFORME IMPLEMENTACION SOFTWARE GLPI	Proceso de bienes y servicios del Concejo Municipal de Yumbo
4. Brindar apoyo a la corporación implementando herramientas colaborativas que permitan el control de la información de los procesos	Se realizo informe relacionado con la implementación de servicio NAS como herramienta colaborativa para el Concejo Municipal de Yumbo	INFORME NAS COMO HERRAMIENTA COLABARATIVA	Proceso de bienes y servicios del Concejo Municipal de Yumbo
OBSERVACIONES			

Cumplimiento de Actividades Contratadas y Objeto Contractual en el Periodo	SI	X	NO		Cumple Parcialmente	

3. SEGUIMIENTO CONTABLE, FINANCIERO Y JURIDICO

	No.	Cuenta / Apropiación	Fecha	Valor
CDP	000036	2.1.2. 02 02 008	02 de febrero de 2023	$ 38.500.000
Registro Presupuestal	000023	2.1.2. 02 02 008	01 de febrero de 2023	$ 38.500.000

Valor a Pagar en el Periodo	Valor Ejecutado a la Fecha	Valor por Ejecutar
$ 3.500.000	$ 38.500.000	$ 0

Prorroga / Adiciones al Contrato: Tiempo ____ Valor: _____ Actividades: _____

Diligenciar en caso de adiciones por valor

Pago de Seguridad Social

Base de Cotización	Valor pagado a			Total, Pagado	Fecha de pago
	EPS	PENSIÓN	ARL		
$ 1,570,000	$ 196.300	$ 251.200	$ 38.300	$ 441.800	05/12/23

4. CERTIFICACIÓN:

a. Por parte del Supervisor:

Certificó el cumplimiento a satisfacción de las obligaciones establecidas en el contrato por parte del contratista en desarrollo de las actividades específicas descritas en el informe de gestión correspondientes al mes de diciembre de 2023 según lo pactado en el contrato en mención del año avante, informe que se anexa debidamente refrendado por las partes. Igualmente se anexa pago de la seguridad social.

b. Por parte del Contratista

Manifiesto bajo la gravedad del juramento que me encuentro afiliado al Sistema de Seguridad Social Integrado, y que realizaré los aportes al mismo, de conformidad con lo dispuesto en el Art. 3.2.7.6 del Decreto 1273 de 2018.

Para constancia de lo anterior se firma la presente acta por el contratista y los que en ella supervisan a los 26 días del mes de diciembre de año 2023.

Firma de Supervisor:
Nombre: MARISOL HERNANDEZ SANCHEZ
Cargo: secretaria general.
Concejo Municipal.

Firma del Contratista:
Nombre: JULIO POTOSI GUAMPE
Documento Identidad: 4.664.904

INFORMACION GENERAL	
FECHA:	18-12-2023
PROCESO:	BIENES Y SERVICIOS
NOMBRE DEL INFORME:	INFORME NAS COMO HERRAMIENTA COLABARATIVA
PRESENTADO POR:	JULIO POTOSÍ GUAMPE
PRESENTADO A:	MARISOL HERNANDEZ SANCHEZ

1. OBJETIVO

Facilitar la administración y colaboración eficiente en la gestión de información. Este sistema permitirá a los usuarios compartir información almacenada en carpetas compartidas a través de un proceso de autenticación seguro.

2. ALCANCE

La implementación abarcará las siguientes áreas y funcionalidades:

- **Autenticación Segura:**

Establecimiento de un sistema de autenticación robusto para garantizar la seguridad de acceso a las carpetas compartidas.

- **Carpetas Compartidas:**

Creación de carpetas compartidas para la colaboración en documentos e información relevante.

Definición de permisos y accesos específicos para cada usuario o grupo.

- **Gestión de Información:**

Facilitar la carga, descarga y actualización de documentos de manera centralizada.

Implementación de un sistema de versionado para un seguimiento eficiente de cambios.

3. DESARROLLO DEL INFORME

3.1. Evaluación de Necesidades:

Se realizó un análisis exhaustivo de los requisitos del Concejo Municipal de Yumbo, identificando la necesidad de una solución centralizada para la gestión y colaboración de documentos.

3.2. Selección de Servicios NAS:

Después de una cuidadosa evaluación, se seleccionaron servicios NAS como la solución más adecuada, considerando su capacidad de proporcionar almacenamiento compartido seguro y administración eficiente.

3.3. Implementación:

La implementación se llevó a cabo de manera escalonada, asegurando la configuración adecuada de la autenticación y la creación de carpetas compartidas. Se brindó capacitación al personal sobre el uso efectivo de la plataforma.

3.4. Integración con Procesos Actuales:

La solución se integró con los procesos existentes del Concejo Municipal, permitiendo una transición sin problemas y minimizando la interrupción en las operaciones diarias.

4. RECOMENDACIONES:

- Fomentar el uso activo de las carpetas compartidas entre los equipos.
- Realizar sesiones de formación periódicas para garantizar un uso efectivo de la plataforma.
- Mantener políticas de seguridad de datos y realizar auditorías regulares.

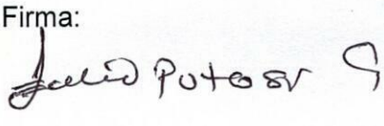
5. CONCLUSIONES:

La implementación de servicios NAS ha mejorado la colaboración y la gestión de información en el Concejo Municipal de Yumbo. La capacidad de compartir documentos de manera segura y eficiente contribuirá a una mayor productividad y coordinación entre los diferentes departamentos.

6. PRÓXIMOS PASOS:

- Monitorear la adopción y el rendimiento del sistema.
- Evaluar la posibilidad de expandir la implementación a otras áreas funcionales.
- Mantenerse actualizado con las actualizaciones de seguridad y características de la plataforma.

Este informe ejecutivo resalta los beneficios obtenidos a través de la implementación de servicios NAS, proporciona recomendaciones para optimizar su uso y sugiere posibles pasos futuros para mejorar aún más la eficiencia operativa.

Elaborado por: Julio Potosí Guampe	Contratista: Ingeniero Informático	Firma: 

INFORMACION GENERAL	
FECHA:	18-12-2023
PROCESO:	BIENES Y SERVICIOS
NOMBRE DEL INFORME:	INFORME IMPLEMENTACION SOFTWARE GLPI
PRESENTADO POR:	JULIO POTOSÍ GUAMPE
PRESENTADO A:	MARISOL HERNANDEZ SANCHEZ

1. OBJETIVO

mejorar la eficiencia y eficacia de las operaciones de soporte técnico, gestión de inventario de equipos, y administración de usuarios y grupos. Este sistema busca optimizar la atención de casos relacionados con el soporte técnico, asegurando un entorno tecnológico más organizado y gestionado.

2. ALCANCE

La implementación abarcará las siguientes áreas y funcionalidades:

Soporte Técnico:

- Registro centralizado de tickets de soporte.
- Seguimiento y asignación eficiente de casos.
- Comunicación transparente entre usuarios y técnicos.

Inventario de Equipos:

- Identificación y catalogación de todos los equipos.
- Gestión de activos, incluyendo detalles técnicos y ubicación.
- Control de versiones de software y actualizaciones.

Administración de Usuarios y Grupos:

- Creación y gestión de perfiles de usuario.
- Asignación y manejo de permisos.
- Manejo de grupos para una administración más eficiente..

3. DESARROLLO DEL INFORME

3.1. Evaluación de Necesidades:

Se llevó a cabo un análisis detallado de los requerimientos del Concejo Municipal de Yumbo, identificando las principales necesidades en términos de soporte técnico, inventario de equipos y administración de usuarios.

3.2. Selección de GLPI:

Se seleccionó GLPI como la solución más adecuada para satisfacer las necesidades identificadas. Se consideraron sus capacidades de seguimiento de incidencias, gestión de inventario y administración de usuarios, así como su capacidad de personalización.

3.3. Implementación:

La implementación se realizó en fases, abordando primero el módulo de soporte técnico, seguido del inventario de equipos y finalmente la administración de usuarios y grupos. Se llevaron a cabo capacitaciones para el personal involucrado.

3.4. Integración con Procesos Actuales:

GLPI se integró de manera fluida con los procesos actuales del Concejo Municipal, minimizando interrupciones y facilitando una transición suave.

4. RECOMENDACIONES:

- Mantener sesiones regulares de capacitación para el personal.
- Realizar auditorías periódicas del inventario para garantizar precisión.
- Promover la adopción activa del sistema por parte de todos los usuarios involucrados.

5. CONCLUSIONES:

La implementación exitosa de GLPI ha mejorado significativamente la eficiencia operativa del Concejo Municipal de Yumbo en términos de soporte técnico, gestión de inventario y administración de usuarios. Se espera que esto conduzca a una mayor productividad y satisfacción del usuario.

6. PRÓXIMOS PASOS:

- Monitorear continuamente el rendimiento del sistema.
- Realizar actualizaciones regulares de software según las recomendaciones del proveedor.
- Evaluar la posibilidad de expandir el uso de GLPI para otras áreas operativas.
- Este informe ejecutivo resume la implementación exitosa del software GLPI, destacando sus beneficios y proporcionando recomendaciones para mantener y mejorar la eficiencia a lo largo del tiempo.

Elaborado por: Julio Potosí Guampe	Contratista: Ingeniero Informático	Firma:

Tabla de contenido

1. INTRODUCCION 2
2. PLANTEAMIENTO DEL PROBLEMA 3
3. JUSTIFICACION 4
4. OBJETIVO GENERAL 5
5. OBJETIVOS ESPECÍFICO 5
6. ALCANCE Y COBERTURA 6
7. IDENTIFICACION Y ANALISI DE RIESGO 7
8. DESCRIPCIÓN Y ANÁLISIS DE RIESGOS 14

1. INTRODUCCION

En la actualidad, la información es un activo esencial para las organizaciones, tanto públicas como privadas. La información puede ser utilizada para una variedad de propósitos, incluyendo la toma de decisiones, la prestación de servicios y la innovación.

La protección de la información es fundamental para garantizar el funcionamiento efectivo de las organizaciones. La información puede ser vulnerable a una variedad de amenazas, incluyendo el acceso no autorizado, la modificación, la destrucción o la pérdida.

El Concejo Municipal de Yumbo es una entidad pública que procesa una gran cantidad de información sensible. La información procesada por el Concejo incluye información personal de los ciudadanos, información financiera y información sobre el funcionamiento de la entidad.

La protección de la información del Concejo Municipal de Yumbo es esencial para garantizar la confianza de los ciudadanos y para el buen funcionamiento de la entidad.

2. PLANTEAMIENTO DEL PROBLEMA

En un mundo interconectado y dependiente de la tecnología, el Concejo Municipal de Yumbo enfrenta desafíos significativos en la protección de la información crítica. Las amenazas cibernéticas, la pérdida accidental de datos y otros riesgos inherentes a la gestión de la información exigen una respuesta estratégica y proactiva. La falta de un marco robusto de seguridad y privacidad expone al Concejo a posibles violaciones de la confidencialidad, la integridad y la disponibilidad de datos, comprometiendo la eficacia de las operaciones y socavando la confianza de la ciudadanía.

3. JUSTIFICACION

La implementación de un Plan de Privacidad y Seguridad de la Información se justifica por la necesidad de resguardar los intereses de los ciudadanos y garantizar la integridad de los procesos administrativos. Además, en un contexto legal cada vez más riguroso en materia de protección de datos personales, el cumplimiento normativo se erige como un imperativo. La justificación de este plan radica también en la preservación de la reputación institucional, ya que la confianza ciudadana es un activo fundamental. Solo a través de medidas adecuadas y continuas de seguridad de la información podemos garantizar una gestión transparente y eficiente de los recursos públicos.

4. OBJETIVO GENERAL

Garantizar la confidencialidad, integridad y disponibilidad de la información del Concejo Municipal de Yumbo, asegurando la protección de los datos sensibles y la continuidad de las operaciones.

5. OBJETIVOS ESPECÍFICO

Los objetivos específicos del plan son los siguientes:

- Identificar y evaluar los riesgos de privacidad y seguridad de la información de la entidad.
- Implementar controles de seguridad para mitigar los riesgos identificados.
- Educar y concientizar a los empleados sobre la importancia de la privacidad y seguridad de la información.

6. ALCANCE Y COBERTURA

El plan aplica a toda la información de la entidad, incluyendo la información física, digital y en tránsito. El plan cubre todos los procesos y servicios de la entidad que involucran el tratamiento de información.

7. IDENTIFICACION Y ANALISI DE RIESGO

7.1. Proceso de identificación de activos de información

Objetivo: Identificar todos los activos de información de la entidad, incluyendo su clasificación, ubicación y valor.

Alcance: El proceso debe aplicarse a toda la información de la entidad, incluyendo la información física, digital y en tránsito.

Responsables: El proceso debe ser liderado por el responsable de la seguridad de la información, con la participación de todos los empleados de la entidad.

Pasos:

1. Definición de criterios de inclusión: Los criterios de inclusión deben definir qué se considera un activo de información para el propósito del proceso. Los criterios pueden incluir el tipo de información, la sensibilidad de la información, la importancia de la información para la entidad, etc.
2. Recolección de información: La información sobre los activos de información puede ser recopilada de una variedad de fuentes, incluyendo:
    - Inventarios de activos
    - Documentación técnica
    - Entrevistas con empleados
    - Auditorías
3. Clasificación de activos: Los activos de información deben ser clasificados en función de su sensibilidad y valor. La clasificación puede ayudar a determinar los controles de seguridad necesarios para proteger los activos.
4. Ubicación de activos: Los activos de información deben ser ubicados para facilitar su identificación y protección.
5. Valoración de activos: Los activos de información deben ser valorados para determinar su importancia para la entidad. La valoración puede ayudar a determinar los recursos que se deben invertir en su protección.

Herramientas y técnicas:

- Software de gestión de activos de información
- Herramientas de auditoría de seguridad
- Entrevistas con empleados

Documentación:

- Lista de activos de información
- Clasificación de activos de información
- Ubicación de activos de información
- Valoración de activos de información

Metodología

El proceso de identificación de activos de información puede realizarse mediante una variedad de métodos, incluyendo:

- Revisión documental: Revisión de documentos, políticas y procedimientos para identificar la información que se trata o almacena.
- Entrevistas con empleados: Entrevistas con empleados para identificar la información que utilizan en su trabajo.
- Inspección física: Inspección física de las instalaciones de la organización para identificar la información física.

Resultados

El resultado del proceso de identificación de activos de información es un inventario de activos de información. Este inventario debe incluir la siguiente información para cada activo de información:

- Nombre del activo de información.
- Tipo de activo de información.
- Ubicación del activo de información.

- Clasificación del activo de información.
- Valor del activo de información.

Recomendaciones

Se recomienda que el proceso de identificación de activos de información se realice al menos una vez al año, o con mayor frecuencia si es necesario. También se recomienda que el inventario de activos de información se mantenga actualizado para reflejar los cambios en la información que utiliza la organización.

7.2. Identificación de amenazas y vulnerabilidades.

Proceso de evaluación de la importancia de los procesos

El proceso de evaluación de la importancia de los procesos es el segundo paso en la gestión de riesgos de privacidad y seguridad de la información. Este proceso tiene como objetivo identificar los procesos que son críticos para la organización y que, por lo tanto, deben protegerse de manera especial.

Objetivo

El objetivo del proceso de evaluación de la importancia de los procesos es identificar los procesos que son críticos para la organización, teniendo en cuenta los siguientes factores:

- La importancia de la información que se trata en el proceso.
- El impacto potencial de una interrupción del proceso.
- La dependencia de otros procesos.

Alcance

El proceso de evaluación de la importancia de los procesos debe aplicarse a todos los procesos de la organización, incluyendo:

- Los procesos que tratan información confidencial.
- Los procesos que son críticos para el funcionamiento de la organización.
- Los procesos que son interdependientes de otros procesos.

Responsabilidades

El proceso de evaluación de la importancia de los procesos es responsabilidad del responsable de la seguridad de la información. Sin embargo, es importante que el proceso involucre a los empleados de todos los niveles de la organización, ya que ellos son los que tienen un mejor conocimiento de los procesos que se llevan a cabo en la organización.

Metodología

El proceso de evaluación de la importancia de los procesos puede realizarse mediante una variedad de métodos, incluyendo:

- Revisión documental: Revisión de documentos, políticas y procedimientos para identificar los procesos que se llevan a cabo en la organización.
- Entrevistas con empleados: Entrevistas con empleados para identificar los procesos que son críticos para el funcionamiento de la organización.
- Análisis de datos: Análisis de datos históricos para identificar los procesos que han sido más afectados por interrupciones o fallos.

Resultados

El resultado del proceso de evaluación de la importancia de los procesos es una matriz de importancia de procesos. Esta matriz debe incluir la siguiente información para cada proceso:

- Nombre del proceso.
- Descripción del proceso.
- Clasificación de la importancia del proceso.

Recomendaciones

Se recomienda que el proceso de evaluación de la importancia de los procesos se realice al menos una vez al año, o con mayor frecuencia si es necesario. También se recomienda que la matriz de importancia de procesos se mantenga actualizada para reflejar los cambios en los procesos que se llevan a cabo en la organización.

7.3. Estimación de los impactos potenciales de los riesgos.

Proceso de estimación de los impactos potenciales de los riesgos

El proceso de estimación de los impactos potenciales de los riesgos es el tercer paso en la gestión de riesgos de privacidad y seguridad de la información. Este proceso tiene como objetivo identificar el impacto potencial que podría tener un riesgo si se materializa.

Objetivo

El objetivo del proceso de estimación de los impactos potenciales de los riesgos es identificar el impacto potencial que podría tener un riesgo si se materializa.

Alcance

El proceso de estimación de los impactos potenciales de los riesgos debe aplicarse a todos los riesgos identificados en el proceso de identificación de riesgos.

Responsabilidades

El proceso de estimación de los impactos potenciales de los riesgos es responsabilidad del responsable de la seguridad de la información. Sin embargo, es importante que el proceso involucre a los empleados de todos los niveles de la organización, ya que ellos son los que tienen un mejor conocimiento de los riesgos potenciales.

Metodología

El proceso de estimación de los impactos potenciales de los riesgos puede realizarse mediante una variedad de métodos, incluyendo:

- Análisis de impacto en el negocio: Este método se utiliza para estimar el impacto que un riesgo podría tener en los objetivos de negocio de la organización.
- Análisis de impacto en la organización: Este método se utiliza para estimar el impacto que un riesgo podría tener en la organización en su conjunto.
- Análisis de impacto en los individuos: Este método se utiliza para estimar el impacto que un riesgo podría tener en los individuos, como los empleados, los clientes o los ciudadanos.

Resultados

El resultado del proceso de estimación de los impactos potenciales de los riesgos es una lista de riesgos con sus respectivos impactos potenciales. Esta lista debe incluir la siguiente información para cada riesgo:

- Nombre del riesgo.
- Descripción del riesgo.
- Impacto potencial del riesgo.

Recomendaciones

Se recomienda que el proceso de estimación de los impactos potenciales de los riesgos se realice al menos una vez al año, o con mayor frecuencia si es necesario.

7.4. Calificación de los riesgos.

Proceso de calificación de los riesgos

El proceso de calificación de los riesgos es el cuarto paso en la gestión de riesgos de privacidad y seguridad de la información. Este proceso tiene como objetivo determinar el nivel de riesgo de cada riesgo identificado.

Objetivo

El objetivo del proceso de calificación de los riesgos es determinar el nivel de riesgo de cada riesgo identificado.

Alcance

El proceso de calificación de los riesgos debe aplicarse a todos los riesgos identificados en la organización.

Responsabilidades

El proceso de calificación de los riesgos es responsabilidad del responsable de la seguridad de la información. Sin embargo, es importante que el proceso involucre a los empleados de todos los niveles de la organización, ya que ellos son los que tienen un mejor conocimiento de los procesos y activos de información que podrían verse afectados por los riesgos.

Metodología

El proceso de calificación de los riesgos puede realizarse mediante una variedad de métodos, incluyendo:

- Método cualitativo: Evaluación subjetiva del nivel de riesgo, utilizando una escala de calificación.
- Método cuantitativo: Evaluación objetiva del nivel de riesgo, utilizando métodos matemáticos.

Resultados

El resultado del proceso de calificación de los riesgos es una lista de riesgos calificados. Esta lista debe incluir la siguiente información para cada riesgo:

- Nombre del riesgo.
- Probabilidad de ocurrencia del riesgo.
- Impacto potencial del riesgo.
- Nivel de riesgo del riesgo.

Recomendaciones

Se recomienda que el proceso de calificación de los riesgos se realice al menos una vez al año, o con mayor frecuencia si es necesario.

8. DESCRIPCIÓN Y ANÁLISIS DE RIESGOS

La descripción y análisis de riesgos se llevará a cabo mediante un proceso que incluya los siguientes pasos:

8.1. Descripción de los riesgos.

Proceso de descripción de los riesgos

El proceso de descripción de los riesgos es el primer paso en la descripción y análisis de riesgos de privacidad y seguridad de la información. Este proceso tiene como objetivo identificar y describir los riesgos que podrían afectar a la organización.

Objetivo

El objetivo del proceso de descripción de los riesgos es identificar y describir los riesgos que podrían afectar a la organización.

Alcance

El proceso de descripción de los riesgos debe aplicarse a todos los activos de información de la organización, incluyendo la información física, digital y en tránsito.

Responsabilidades

El proceso de descripción de los riesgos es responsabilidad del responsable de la seguridad de la información. Sin embargo, es importante que el proceso involucre a los empleados de todos los niveles de la organización, ya que ellos son los que tienen un mejor conocimiento de los activos de información que podrían verse afectados por los riesgos.

Metodología

El proceso de descripción de los riesgos puede realizarse mediante una variedad de métodos, incluyendo:

- Revisión documental: Revisión de documentos, políticas y procedimientos para identificar los riesgos.
- Entrevistas con empleados: Entrevistas con empleados para identificar los riesgos.
- Workshops: Workshops con empleados para identificar los riesgos.

Resultados

El resultado del proceso de descripción de los riesgos es una lista de riesgos identificados. Esta lista debe incluir la siguiente información para cada riesgo:

- Nombre del riesgo.
- Descripción del riesgo.
- Causas del riesgo.
- Consecuencias del riesgo.

Recomendaciones

Se recomienda que el proceso de descripción de los riesgos se realice al menos una vez al año, o con mayor frecuencia si es necesario.

8.2. Análisis de las causas y consecuencias de los riesgos.

Proceso de análisis de las causas y consecuencias de los riesgos

El proceso de análisis de las causas y consecuencias de los riesgos es el segundo paso en la descripción y análisis de riesgos de privacidad y seguridad de la información. Este proceso tiene como objetivo comprender mejor los riesgos identificados, identificando sus causas y consecuencias potenciales.

Objetivo

El objetivo del proceso de análisis de las causas y consecuencias de los riesgos es comprender mejor los riesgos identificados, identificando sus causas y consecuencias potenciales.

Alcance

El proceso de análisis de las causas y consecuencias de los riesgos debe aplicarse a todos los riesgos identificados en la organización.

Responsabilidades

El proceso de análisis de las causas y consecuencias de los riesgos es responsabilidad del responsable de la seguridad de la información. Sin embargo, es importante que el proceso involucre a los empleados de todos los niveles de la organización, ya que ellos son los que tienen un mejor conocimiento de los activos de información que podrían verse afectados por los riesgos.

Metodología

El proceso de análisis de las causas y consecuencias de los riesgos puede realizarse mediante una variedad de métodos, incluyendo:

- Revisión documental: Revisión de documentos, políticas y procedimientos para identificar las causas y consecuencias de los riesgos.
- Entrevistas con empleados: Entrevistas con empleados para identificar las causas y consecuencias de los riesgos.
- Workshops: Workshops con empleados para identificar las causas y consecuencias de los riesgos.

Resultados

El resultado del proceso de análisis de las causas y consecuencias de los riesgos es una lista de riesgos identificados, con información adicional sobre sus causas y consecuencias potenciales. Esta lista debe incluir la siguiente información para cada riesgo:

- Nombre del riesgo.
- Descripción del riesgo.
- Causas del riesgo.
- Consecuencias del riesgo.

- Probabilidad de ocurrencia del riesgo.
- Impacto potencial del riesgo.

Recomendaciones

Se recomienda que el proceso de análisis de las causas y consecuencias de los riesgos se realice al menos una vez al año, o con mayor frecuencia si es necesario.

8.3. Recomendaciones para la mitigación de los riesgos.

Proceso de recomendaciones para la mitigación de los riesgos

El proceso de recomendaciones para la mitigación de los riesgos es el tercer paso en la descripción y análisis de riesgos de privacidad y seguridad de la información. Este proceso tiene como objetivo identificar las medidas que se pueden tomar para mitigar los riesgos identificados, reduciendo su probabilidad de ocurrencia o su impacto potencial.

Objetivo

El objetivo del proceso de recomendaciones para la mitigación de los riesgos es identificar las medidas que se pueden tomar para mitigar los riesgos identificados, reduciendo su probabilidad de ocurrencia o su impacto potencial.

Alcance

El proceso de recomendaciones para la mitigación de los riesgos debe aplicarse a todos los riesgos identificados en la organización.

Responsabilidades

El proceso de recomendaciones para la mitigación de los riesgos es responsabilidad del responsable de la seguridad de la información. Sin embargo, es importante que el proceso involucre a los empleados de todos los niveles de la organización, ya que ellos son los que tienen un mejor conocimiento de los activos de información que podrían verse afectados por los riesgos.

Metodología

El proceso de recomendaciones para la mitigación de los riesgos puede realizarse mediante una variedad de métodos, incluyendo:

- Revisión documental: Revisión de documentos, políticas y procedimientos para identificar medidas de mitigación de riesgos.
- Entrevistas con empleados: Entrevistas con empleados para identificar medidas de mitigación de riesgos.
- Workshops: Workshops con empleados para identificar medidas de mitigación de riesgos.

Resultados

El resultado del proceso de recomendaciones para la mitigación de los riesgos es un conjunto de recomendaciones para mitigar los riesgos identificados. Estas recomendaciones deben incluir la siguiente información para cada riesgo:

- Nombre del riesgo.
- Recomendación para mitigar el riesgo.
- Explicación de la recomendación.
- Costo estimado de la recomendación.
- Tiempo estimado para implementar la recomendación.

Recomendaciones

Se recomienda que el proceso de recomendaciones para la mitigación de los riesgos se realice al menos una vez al año, o con mayor frecuencia si es necesario.

8.4. Identificación de procesos críticos

Proceso de identificación de procesos críticos

El proceso de identificación de procesos críticos es el cuarto paso en la descripción y análisis de riesgos de privacidad y seguridad de la información. Este proceso tiene como objetivo identificar los procesos que son esenciales para la organización y que, por lo tanto, deben ser protegidos de los riesgos.

Objetivo

El objetivo del proceso de identificación de procesos críticos es identificar los procesos que son esenciales para la organización y que, por lo tanto, deben ser protegidos de los riesgos.

Alcance

El proceso de identificación de procesos críticos debe aplicarse a todos los procesos de la organización, incluyendo los procesos de negocio, los procesos de apoyo y los procesos de TI.

Responsabilidades

El proceso de identificación de procesos críticos es responsabilidad del responsable de la seguridad de la información. Sin embargo, es importante que el proceso involucre a los empleados de todos los niveles de la organización, ya que ellos son los que tienen un mejor conocimiento de los procesos de la organización.

Metodología

El proceso de identificación de procesos críticos puede realizarse mediante una variedad de métodos, incluyendo:

- Revisión documental: Revisión de documentos, políticas y procedimientos para identificar los procesos críticos.
- Entrevistas con empleados: Entrevistas con empleados para identificar los procesos críticos.
- Workshops: Workshops con empleados para identificar los procesos críticos.

Resultados

El resultado del proceso de identificación de procesos críticos es una lista de procesos críticos. Esta lista debe incluir la siguiente información para cada proceso:

- Nombre del proceso.
- Descripción del proceso.

- Importancia del proceso para la organización.

Recomendaciones

Se recomienda que el proceso de identificación de procesos críticos se realice al menos una vez al año, o con mayor frecuencia si es necesario.

9. FACTORES CRÍTICOS PARA CONSIDERAR

9.1. Identificación de los procesos de la entidad.

El proceso de identificación de los procesos de la entidad es el primer paso en la identificación de procesos críticos. Este proceso tiene como objetivo identificar todos los procesos que se realizan en la organización, incluyendo los procesos de negocio, los procesos de apoyo y los procesos de TI.

Objetivo

El objetivo del proceso de identificación de los procesos de la entidad es identificar todos los procesos que se realizan en la organización, incluyendo los procesos de negocio, los procesos de apoyo y los procesos de TI.

Alcance

El proceso de identificación de los procesos de la entidad debe aplicarse a todos los procesos de la organización, sin importar su tamaño o complejidad.

Responsabilidades

El proceso de identificación de los procesos de la entidad es responsabilidad del responsable de la seguridad de la información. Sin embargo, es importante que el proceso involucre a los empleados de todos los niveles de la organización, ya que ellos son los que tienen un mejor conocimiento de los procesos de la organización.

Metodología

El proceso de identificación de los procesos de la entidad puede realizarse mediante una variedad de métodos, incluyendo:

- Revisión documental: Revisión de documentos, políticas y procedimientos para identificar los procesos.
- Entrevistas con empleados: Entrevistas con empleados para identificar los procesos.
- Workshops: Workshops con empleados para identificar los procesos.

Resultados

El resultado del proceso de identificación de los procesos de la entidad es una lista de procesos de la entidad. Esta lista debe incluir la siguiente información para cada proceso:

- Nombre del proceso.
- Descripción del proceso.
- Entradas y salidas del proceso.
- Responsables del proceso.

Recomendaciones

Se recomienda que el proceso de identificación de los procesos de la entidad se realice al menos una vez al año, o con mayor frecuencia si es necesario.

9.2. Evaluación de la importancia de los procesos.

Proceso de identificación de los procesos de la entidad

El proceso de identificación de los procesos de la entidad es el primer paso en la identificación de procesos críticos. Este proceso tiene como objetivo identificar todos los procesos que se realizan en la organización, incluyendo los procesos de negocio, los procesos de apoyo y los procesos de TI.

Objetivo

El objetivo del proceso de identificación de los procesos de la entidad es identificar todos los procesos que se realizan en la organización, incluyendo los procesos de negocio, los procesos de apoyo y los procesos de TI.

Alcance

El proceso de identificación de los procesos de la entidad debe aplicarse a todos los procesos de la organización, sin importar su tamaño o complejidad.

Responsabilidades

El proceso de identificación de los procesos de la entidad es responsabilidad del responsable de la seguridad de la información. Sin embargo, es importante que el proceso involucre a los empleados de todos los niveles de la organización, ya que ellos son los que tienen un mejor conocimiento de los procesos de la organización.

Metodología

El proceso de identificación de los procesos de la entidad puede realizarse mediante una variedad de métodos, incluyendo:

- Revisión documental: Revisión de documentos, políticas y procedimientos para identificar los procesos.
- Entrevistas con empleados: Entrevistas con empleados para identificar los procesos.
- Workshops: Workshops con empleados para identificar los procesos.

Resultados

El resultado del proceso de identificación de los procesos de la entidad es una lista de procesos de la entidad. Esta lista debe incluir la siguiente información para cada proceso:

- Nombre del proceso.
- Descripción del proceso.
- Entradas y salidas del proceso.

- Responsables del proceso.

Recomendaciones

Se recomienda que el proceso de identificación de los procesos de la entidad se realice al menos una vez al año, o con mayor frecuencia si es necesario.

9.3. Identificación de los procesos críticos.

Proceso de identificación de los procesos de la entidad

El proceso de identificación de los procesos de la entidad es el primer paso en la identificación de procesos críticos. Este proceso tiene como objetivo identificar todos los procesos que se realizan en la organización, incluyendo los procesos de negocio, los procesos de apoyo y los procesos de TI.

Objetivo

El objetivo del proceso de identificación de los procesos de la entidad es identificar todos los procesos que se realizan en la organización, incluyendo los procesos de negocio, los procesos de apoyo y los procesos de TI.

Alcance

El proceso de identificación de los procesos de la entidad debe aplicarse a todos los procesos de la organización, sin importar su tamaño o complejidad.

Responsabilidades

El proceso de identificación de los procesos de la entidad es responsabilidad del responsable de la seguridad de la información. Sin embargo, es importante que el proceso involucre a los empleados de todos los niveles de la organización, ya que ellos son los que tienen un mejor conocimiento de los procesos de la organización.

Metodología

El proceso de identificación de los procesos de la entidad puede realizarse mediante una variedad de métodos, incluyendo:

- Revisión documental: Revisión de documentos, políticas y procedimientos para identificar los procesos.
- Entrevistas con empleados: Entrevistas con empleados para identificar los procesos.
- Workshops: Workshops con empleados para identificar los procesos.

Resultados

El resultado del proceso de identificación de los procesos de la entidad es una lista de procesos de la entidad. Esta lista debe incluir la siguiente información para cada proceso:

- Nombre del proceso.
- Descripción del proceso.
- Entradas y salidas del proceso.
- Responsables del proceso.

Recomendaciones

Se recomienda que el proceso de identificación de los procesos de la entidad se realice al menos una vez al año, o con mayor frecuencia si es necesario.

10. NIVELES DE PRIORIDAD Y CRITICIDAD DE LOS RECURSOS INFORMÁTICOS

La importancia de la información almacenada o procesada por un recurso informático es un factor clave para determinar su nivel de prioridad y criticidad. La información puede ser importante por una variedad de razones, incluyendo:

- Su valor económico: La información puede tener un valor económico significativo, como en el caso de datos de clientes, datos financieros o datos de propiedad intelectual.
- Su valor legal: La información puede tener un valor legal, como en el caso de registros médicos, registros financieros o registros de cumplimiento normativo.

- Su valor estratégico: La información puede tener un valor estratégico para la organización, como en el caso de información de investigación y desarrollo, información de marketing o información de planificación.

Los recursos informáticos que almacenan o procesan información importante deben tener un nivel de prioridad y criticidad alto. Esto se debe a que la pérdida o el acceso no autorizado a esta información podría tener un impacto significativo en la organización.

10.1. La importancia de la información almacenada o procesada por el recurso

La importancia de la información almacenada o procesada por un recurso informático es un factor clave para determinar su nivel de prioridad y criticidad. La información puede ser importante por una variedad de razones, incluyendo:

- Su valor económico: La información puede tener un valor económico significativo, como en el caso de datos de clientes, datos financieros o datos de propiedad intelectual.
- Su valor legal: La información puede tener un valor legal, como en el caso de registros médicos, registros financieros o registros de cumplimiento normativo.
- Su valor estratégico: La información puede tener un valor estratégico para la organización, como en el caso de información de investigación y desarrollo, información de marketing o información de planificación.

Los recursos informáticos que almacenan o procesan información importante deben tener un nivel de prioridad y criticidad alto. Esto se debe a que la pérdida o el acceso no autorizado a esta información podría tener un impacto significativo en la organización.

Recomendaciones

Para determinar la importancia de la información almacenada o procesada por un recurso informático, se recomienda considerar los siguientes factores:

- El valor económico de la información.
- El valor legal de la información.

- El valor estratégico de la información.

Esta información se puede recopilar mediante una variedad de métodos, incluyendo:

- Revisión documental: Revisión de documentos, políticas y procedimientos para identificar la información almacenada o procesada por el recurso.
- Entrevistas con empleados: Entrevistas con empleados para identificar la información almacenada o procesada por el recurso.
- Workshops: Workshops con empleados para identificar la información almacenada o procesada por el recurso.

10.2. El impacto potencial de una pérdida o daño del recurso.

El impacto potencial de una pérdida o daño del recurso es otro factor clave para determinar su nivel de prioridad y criticidad. El impacto potencial puede ser medido en términos de los siguientes factores:

- Costos: Los costos asociados con la pérdida o el daño del recurso, incluyendo los costos de restauración, los costos de interrupción del negocio y los costos de reputación.
- Tiempo: El tiempo que tardaría la organización en recuperarse de la pérdida o el daño del recurso.
- Operaciones: El impacto de la pérdida o el daño del recurso en las operaciones de la organización.
- Regulación: El impacto de la pérdida o el daño del recurso en el cumplimiento normativo de la organización.

Los recursos informáticos que tienen un impacto potencial significativo deben tener un nivel de prioridad y criticidad alto. Esto se debe a que la pérdida o el daño de estos recursos podría tener un impacto significativo en la organización

Recomendaciones

Para determinar el impacto potencial de una pérdida o daño del recurso, se recomienda considerar los siguientes factores:

- Los costos asociados con la pérdida o el daño del recurso.
- El tiempo que tardaría la organización en recuperarse de la pérdida o el daño del recurso.
- El impacto de la pérdida o el daño del recurso en las operaciones de la organización.
- El impacto de la pérdida o el daño del recurso en el cumplimiento normativo de la organización.

Esta información se puede recopilar mediante una variedad de métodos, incluyendo:

- Revisión documental: Revisión de documentos, políticas y procedimientos para identificar los factores que podrían causar la pérdida o el daño del recurso.
- Entrevistas con empleados: Entrevistas con empleados para identificar los factores que podrían causar la pérdida o el daño del recurso.
- Workshops: Workshops con empleados para identificar los factores que podrían causar la pérdida o el daño del recurso.

10.3. El impacto potencial de una interrupción del recurso.

El impacto potencial de una interrupción del recurso

El impacto potencial de una interrupción del recurso es el tercer factor clave para determinar su nivel de prioridad y criticidad. La interrupción del recurso puede ser temporal o permanente, y puede tener una variedad de causas, incluyendo:

- Fallo del hardware o software.
- Ataque cibernético.
- Error humano.
- Desastre natural.

Los recursos informáticos que tienen un impacto potencial significativo en caso de interrupción deben tener un nivel de prioridad y criticidad alto. Esto se debe a que la interrupción de estos recursos podría tener un impacto significativo en la organización.

Recomendaciones

Para determinar el impacto potencial de una interrupción del recurso, se recomienda considerar los siguientes factores:

- La duración de la interrupción.
- El impacto de la interrupción en las operaciones de la organización.
- El impacto de la interrupción en los clientes y socios de la organización.

11. CONCLUSIONES

El plan de privacidad y seguridad de la información es un documento esencial para cualquier organización que quiera proteger su información. Este plan debe ser desarrollado teniendo en cuenta las necesidades específicas de la organización, y debe ser revisado y actualizado periódicamente para garantizar que sigue siendo eficaz.

Los puntos clave que se deben considerar al desarrollar un plan de privacidad y seguridad de la información son los siguientes:

- Identificación de los activos de información: La primera etapa del desarrollo del plan es identificar los activos de información de la organización, incluyendo la información confidencial, sensible o crítica.
- Análisis de riesgos: Una vez que se han identificado los activos de información, es necesario realizar un análisis de riesgos para identificar los posibles riesgos a los que están expuestos.
- Mitigación de riesgos: El siguiente paso es identificar las medidas de mitigación de riesgos que se pueden implementar para reducir la probabilidad o el impacto de los riesgos identificados.
- Asignación de funciones: Las funciones y responsabilidades relacionadas con la privacidad y la seguridad de la información deben ser asignadas a los empleados adecuados.

• Revisado por: • Julio Potosí	Contratista profesional Ingeniero en Sistemas	Julio Potosí Firma:

Tabla de contenido

1. INTRODUCCION 2
2. OBJETIVO GENERAL 3
3. OBJETIVOS ESPECÍFICO 3
4. CONTEXTO ORGANIZACIONAL 4
5. MARCO NORMATIVO 5
6. IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS: 6
7. EVALUACIÓN DE RIESGOS 12
8. MEDIDAS DE MITIGACIÓN 17
9. PLAN DE RESPUESTA A INCIDENTES: 22
10. CONCIENTIZACIÓN Y FORMACIÓN 33
10.1. Fomento de la conciencia sobre la importancia de la seguridad y privacidad de la información 33
11. REVISIÓN Y MEJORA CONTINUA: 34
12. DOCUMENTACIÓN Y REPORTES: 37
13. CONCLUSIONES 41

1. INTRODUCCION

La información es un activo esencial para cualquier organización, y el Concejo Municipal de Yumbo no es una excepción. La información del Concejo Municipal de Yumbo incluye datos personales, financieros, comerciales y de propiedad intelectual, que son confidenciales, sensibles o críticos para el funcionamiento de la entidad.

Los riesgos a los que están expuestos los activos de información del Concejo Municipal de Yumbo son diversos, e incluyen amenazas internas y externas, como:

- Ataques cibernéticos, como el robo de datos, el malware y el ransomware.
- Errores humanos, como la pérdida de datos, la divulgación accidental de información confidencial y la mala configuración de los sistemas.
- Desastres naturales, como incendios, inundaciones y terremotos.

El plan de tratamiento de riesgos del Concejo Municipal de Yumbo tiene como objetivo mitigar estos riesgos y proteger la información de la entidad.

2. OBJETIVO GENERAL

proteger la información confidencial, sensible y crítica de la entidad, garantizando su confidencialidad, integridad y disponibilidad.

3. OBJETIVOS ESPECÍFICO

Los objetivos específicos del plan son los siguientes:

- Identificar y analizar los riesgos a los que están expuestos los activos de información del Concejo Municipal de Yumbo.
- Evaluar la criticidad de los riesgos identificados y priorizar las medidas de mitigación.
- Desarrollar e implementar medidas de mitigación eficaces para reducir la probabilidad o el impacto de los riesgos.
- Establecer un plan de respuesta a incidentes para gestionar los eventos de seguridad que puedan afectar a la información del Concejo Municipal de Yumbo.
- Promover la conciencia y la formación sobre seguridad y privacidad de la información entre el personal del Concejo Municipal de Yumbo

4. CONTEXTO ORGANIZACIONAL

El Concejo Municipal de Yumbo es un organismo público que se encarga de la administración del municipio. La entidad cuenta con una estructura jerárquica, encabezada por el alcalde. El Concejo Municipal de Yumbo cuenta con un equipo de personal que se encarga de las distintas funciones de la entidad.

Los activos de información del Concejo Municipal de Yumbo incluyen los siguientes:

- Datos personales de los empleados, clientes y ciudadanos.
- Datos financieros, como las cuentas bancarias y las transacciones financieras.
- Datos comerciales, como los planes de negocio y las estrategias de marketing.
- Datos de propiedad intelectual, como las patentes y los secretos comerciales.

Los activos de información del Concejo Municipal de Yumbo se almacenan en una variedad de sistemas, incluyendo sistemas informáticos, sistemas de almacenamiento de datos y sistemas físicos, como archivos y documentos.

5. MARCO NORMATIVO

El Concejo Municipal de Yumbo está sujeto a una serie de leyes y regulaciones en materia de privacidad y seguridad de la información. Estas leyes y regulaciones incluyen:

- La Ley 1581 de 2012, que regula el tratamiento de datos personales en Colombia.
- La Ley 1780 de 2016, que establece la seguridad de la información y las TIC.
- El Decreto 1377 de 2013, que regula el uso de la firma electrónica en Colombia.

El plan de tratamiento de riesgos del Concejo Municipal de Yumbo se alinea con estos requisitos legales y normativos.

6. IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS:

6.1. Descripción de la metodología utilizada para identificar y analizar riesgos

La metodología utilizada para identificar y analizar riesgos del Concejo Municipal de Yumbo se basa en los siguientes pasos:

1. Revisión documental: Revisión de documentos, políticas y procedimientos para identificar los activos de información de la entidad y los posibles riesgos a los que están expuestos.
2. Entrevistas con empleados: Entrevistas con empleados para identificar los riesgos a los que están expuestos los activos de información de la entidad.
3. Workshops: Workshops con empleados para identificar los riesgos a los que están expuestos los activos de información de la entidad.

Revisión documental

La revisión documental se centra en los siguientes aspectos:

- Identificación de los activos de información: Los activos de información son los datos, sistemas, aplicaciones y procesos que son importantes para la entidad.
- Identificación de las amenazas: Las amenazas son los eventos o acciones que pueden causar daño a los activos de información.

Entrevistas con empleados

Las entrevistas con empleados se centran en los siguientes aspectos:

- Experiencias personales de los empleados con los riesgos a la seguridad de la información: Los empleados pueden proporcionar información valiosa sobre los riesgos que han experimentado personalmente o que han observado en otros empleados.

Para cada riesgo potencial identificado, se realiza un análisis detallado para determinar su impacto potencial y probabilidad de ocurrencia. El análisis se basa en los siguientes factores:

- Impacto potencial: El impacto potencial de un riesgo se mide en términos de los siguientes aspectos:
  - ❖ Confidencialidad: El impacto en la confidencialidad de la información.
  - ❖ Integridad: El impacto en la integridad de la información.
  - ❖ Disponibilidad: El impacto en la disponibilidad de la información.
- Probabilidad de ocurrencia: La probabilidad de ocurrencia de un riesgo se mide en términos de la siguiente escala:
  - ❖ Alta: El riesgo es muy probable que ocurra.
  - ❖ Media: El riesgo es probable que ocurra.
  - ❖ Baja: El riesgo es poco probable que ocurra.

Conclusiones

La metodología utilizada para identificar y analizar riesgos del Concejo Municipal de Yumbo es un proceso sistemático que permite identificar una gama amplia de riesgos y evaluar su impacto potencial y probabilidad de ocurrencia.

6.2. Listado de riesgos potenciales clasificados por categorías (cibernéticos, físicos, humanos, etc.).

Cibernéticos

- Robo de datos: El robo de datos es un tipo de ataque informático que tiene como objetivo obtener acceso a información confidencial, como datos personales, financieros o comerciales. Este tipo de ataque puede tener un impacto significativo en el Concejo Municipal de Yumbo, ya que podría provocar la pérdida de información confidencial, la interrupción de las operaciones o el daño a la reputación de la entidad.
- Malware: El malware es un software malicioso que se utiliza para dañar o controlar un sistema informático. El malware puede ser utilizado para robar

- Percepción de los empleados sobre los riesgos: Los empleados pueden tener una percepción diferente de los riesgos que los responsables de seguridad de la información.
- Medidas de seguridad que consideran necesarias para mitigar los riesgos: Los empleados pueden proporcionar información sobre las medidas de seguridad que creen que serían más efectivas para mitigar los riesgos.

Workshops

Los workshops se centran en los siguientes aspectos:

- Participación de los empleados: Los workshops permiten fomentar la participación de los empleados y obtener una visión más completa de los riesgos a los que está expuesta la entidad.
- Obtención de información sobre los riesgos: Los workshops permiten obtener información sobre los riesgos a los que están expuestos los activos de información, así como sobre las medidas de seguridad que se consideran necesarias para mitigar los riesgos.

Clasificación de los riesgos

Una vez que se han identificado los riesgos, se clasifican por categorías. Las categorías de riesgos que se utilizan son las siguientes:

- Cibernéticos: Los riesgos cibernéticos son aquellos que se producen a través de un ataque informático. Incluyen riesgos como el robo de datos, el malware, el ransomware y el phishing.
- Físicos: Los riesgos físicos son aquellos que se producen a través de un evento físico. Incluyen riesgos como incendios, inundaciones, terremotos y vandalismo.
- Humanos: Los riesgos humanos son aquellos que se producen por error humano. Incluyen riesgos como la pérdida de datos, la divulgación accidental de información confidencial y la mala configuración de los sistemas.

Análisis de riesgos

datos, dañar archivos o incluso tomar el control de un sistema informático. El Concejo Municipal de Yumbo está expuesto a una variedad de amenazas de malware, como virus, gusanos, troyanos y ransomware.

- Ransomware: El ransomware es un tipo de malware que cifra los datos de un sistema informático y exige un rescate para descifrarlos. El ransomware puede tener un impacto significativo en el Concejo Municipal de Yumbo, ya que podría provocar la pérdida de acceso a los datos, la interrupción de las operaciones o el daño a la reputación de la entidad.
- Phishing: El phishing es un tipo de ataque informático que tiene como objetivo engañar a las personas para que revelen información confidencial, como contraseñas o números de tarjetas de crédito. El Concejo Municipal de Yumbo está expuesto a una variedad de ataques de phishing, ya que los empleados pueden ser víctimas de estos ataques a través del correo electrónico, las redes sociales o los mensajes de texto.

Físicos

- Incendios: Los incendios pueden causar daños significativos a los activos de información del Concejo Municipal de Yumbo, como sistemas informáticos, documentos y archivos. El Concejo Municipal de Yumbo debe contar con un plan de respuesta a incendios para minimizar el impacto de un incendio en sus activos de información.
- Inundaciones: Las inundaciones pueden causar daños significativos a los activos de información del Concejo Municipal de Yumbo, como sistemas informáticos, documentos y archivos. El Concejo Municipal de Yumbo debe contar con un plan de respuesta a inundaciones para minimizar el impacto de una inundación en sus activos de información.
- Terremotos: Los terremotos pueden causar daños significativos a los activos de información del Concejo Municipal de Yumbo, como sistemas informáticos, documentos y archivos. El Concejo Municipal de Yumbo debe contar con un plan de respuesta a terremotos para minimizar el impacto de un terremoto en sus activos de información.
- Vandalismo: El vandalismo puede causar daños significativos a los activos de información del Concejo Municipal de Yumbo, como sistemas informáticos, documentos y archivos. El Concejo Municipal de Yumbo debe contar con un plan de seguridad física para minimizar el riesgo de vandalismo.

Humanos

- Errores humanos: Los errores humanos son una de las principales causas de incidentes de seguridad de la información. Los errores humanos pueden incluir la pérdida de datos, la divulgación accidental de información confidencial y la mala configuración de los sistemas. El Concejo Municipal de Yumbo debe implementar programas de concientización sobre la seguridad de la información para ayudar a reducir el riesgo de errores humanos.
- Mala configuración de los sistemas: Una mala configuración de los sistemas puede crear vulnerabilidades que pueden ser explotadas por los atacantes. El Concejo Municipal de Yumbo debe contar con procesos y procedimientos para garantizar que los sistemas se configuren correctamente.
- Falta de supervisión: La falta de supervisión puede permitir que los empleados realicen actividades que pueden poner en riesgo la seguridad de la información. El Concejo Municipal de Yumbo debe contar con procesos y procedimientos para garantizar que los empleados sean supervisados de forma adecuada

6.3. **Análisis detallado de cada riesgo, incluyendo su impacto potencial y probabilidad de ocurrencia**.

Para cada riesgo potencial identificado, se realiza un análisis detallado para determinar su impacto potencial y probabilidad de ocurrencia. El análisis se basa en los siguientes factores:

- Impacto potencial: El impacto potencial de un riesgo se mide en términos de los siguientes aspectos:
    - ❖ Confidencialidad: El impacto en la confidencialidad de la información.
    - ❖ Integridad: El impacto en la integridad de la información.
    - ❖ Disponibilidad: El impacto en la disponibilidad de la información.
- Probabilidad de ocurrencia: La probabilidad de ocurrencia de un riesgo se mide en términos de la siguiente escala:
    - ❖ Alta: El riesgo es muy probable que ocurra.
    - ❖ Media: El riesgo es probable que ocurra.
    - ❖ Baja: El riesgo es poco probable que ocurra.

Impacto potencial

El impacto potencial de un riesgo se puede determinar considerando los siguientes factores:

- El tipo de información afectada: La información confidencial, como los datos personales, financieros o comerciales, tiene un impacto potencial más significativo que la información no confidencial.
- La cantidad de información afectada: La pérdida de una gran cantidad de información puede tener un impacto potencial más significativo que la pérdida de una pequeña cantidad de información.
- La importancia de la información: La información que es crítica para las operaciones de la entidad tiene un impacto potencial más significativo que la información que no es crítica.

Probabilidad de ocurrencia

La probabilidad de ocurrencia de un riesgo se puede determinar considerando los siguientes factores:

- La frecuencia de los ataques similares: Los riesgos que se han producido con frecuencia en el pasado tienen una probabilidad de ocurrencia más alta.
- La vulnerabilidad de los sistemas: Los sistemas que son vulnerables a los ataques tienen una probabilidad de ocurrencia más alta.
- Los incentivos para los atacantes: Los riesgos que ofrecen un incentivo significativo para los atacantes, como el robo de información confidencial, tienen una probabilidad de ocurrencia más alta.

Riesgo: Robo de datos

Impacto potencial:

- Confidencialidad: La pérdida de datos confidenciales, como datos personales, financieros o comerciales, podría provocar daños a la reputación de la entidad, pérdida de clientes o incluso sanciones legales.
- Integridad: La pérdida de datos puede provocar la corrupción o la modificación de datos, lo que podría dar lugar a errores o fraudes.

- Disponibilidad: La pérdida de acceso a datos críticos podría interrumpir las operaciones de la entidad.

Probabilidad de ocurrencia:

- Frecuencia de ataques similares: Los ataques de robo de datos son comunes y ocurren con frecuencia.
- Vulnerabilidad de los sistemas: Los sistemas informáticos son vulnerables a los ataques de robo de datos, especialmente si no se implementan las medidas de seguridad adecuadas.
- Incentivos para los atacantes: El robo de datos confidenciales puede ofrecer un incentivo significativo para los atacantes, ya que puede ser revendido o utilizado para chantajear a la entidad.

Conclusión:

El riesgo de robo de datos es un riesgo significativo para el Concejo Municipal de Yumbo. El riesgo tiene un impacto potencial alto en todos los aspectos de la información, y la probabilidad de ocurrencia es alta.

7. EVALUACIÓN DE RIESGOS

La evaluación de riesgos es el proceso de determinar la criticidad de los riesgos identificados y priorizar las medidas de mitigación.

Para realizar la evaluación de riesgos para el Concejo Municipal de Yumbo, se recomienda utilizan las siguientes etapas:

1. Clasificación de los riesgos: Los riesgos se clasifican en función de su impacto potencial y probabilidad de ocurrencia.
2. Asignación de niveles de riesgo: A cada riesgo se le asigna un nivel de riesgo en función de su clasificación.
3. Priorización de los riesgos: Los riesgos se priorizan en función de su nivel de riesgo.

Clasificación de los riesgos

Los riesgos se pueden clasificar en función de su impacto potencial y probabilidad de ocurrencia.

- Impacto potencial: El impacto potencial de un riesgo se mide en términos de los siguientes aspectos:
  - ❖ Confidencialidad: El impacto en la confidencialidad de la información.
  - ❖ Integridad: El impacto en la integridad de la información.
  - ❖ Disponibilidad: El impacto en la disponibilidad de la información.
- Probabilidad de ocurrencia: La probabilidad de ocurrencia de un riesgo se mide en términos de la siguiente escala:
  - ❖ Alta: El riesgo es muy probable que ocurra.
  - ❖ Media: El riesgo es probable que ocurra.
  - ❖ Baja: El riesgo es poco probable que ocurra.

Asignación de niveles de riesgo

A cada riesgo se le asigna un nivel de riesgo en función de su clasificación.

- Impacto potencial alto y probabilidad de ocurrencia alta: Riesgo crítico.
- Impacto potencial alto y probabilidad de ocurrencia media: Riesgo alto.
- Impacto potencial alto y probabilidad de ocurrencia baja: Riesgo moderado.
- Impacto potencial medio y probabilidad de ocurrencia alta: Riesgo alto.
- Impacto potencial medio y probabilidad de ocurrencia media: Riesgo moderado.
- Impacto potencial medio y probabilidad de ocurrencia baja: Riesgo bajo.
- Impacto potencial bajo y probabilidad de ocurrencia alta: Riesgo moderado.
- Impacto potencial bajo y probabilidad de ocurrencia media: Riesgo bajo.
- Impacto potencial bajo y probabilidad de ocurrencia baja: Riesgo muy bajo.

Priorización de los riesgos

Los riesgos se priorizan en función de su nivel de riesgo. Los riesgos críticos deben ser mitigados primero, seguidos de los riesgos altos y moderados. Los riesgos bajos y muy bajos pueden ser mitigados posteriormente.

7.1. Establecimiento de un proceso para evaluar y calcular la criticidad de los riesgos identificados

El Concejo Municipal de Yumbo debe establecer un proceso para evaluar y calcular la criticidad de los riesgos identificados. Este proceso debe ser sistemático y objetivo, y debe tener en cuenta los siguientes factores:

- Impacto potencial: El impacto potencial de un riesgo se mide en términos de los siguientes aspectos:
    - ❖ Confidencialidad: El impacto en la confidencialidad de la información.
    - ❖ Integridad: El impacto en la integridad de la información.
    - ❖ Disponibilidad: El impacto en la disponibilidad de la información.
- Probabilidad de ocurrencia: La probabilidad de ocurrencia de un riesgo se mide en términos de la siguiente escala:
    - ❖ Alta: El riesgo es muy probable que ocurra.
    - ❖ Media: El riesgo es probable que ocurra.
    - ❖ Baja: El riesgo es poco probable que ocurra.

El proceso de evaluación de riesgos puede ser manual o automatizado. Si se utiliza un proceso manual, se deben establecer escalas para medir el impacto potencial y la probabilidad de ocurrencia de los riesgos. Si se utiliza un proceso automatizado, se puede utilizar una herramienta de gestión de riesgos que ofrezca estas escalas.

Una vez que se han medido el impacto potencial y la probabilidad de ocurrencia de los riesgos, se puede calcular la criticidad de cada riesgo utilizando la siguiente fórmula:

```
Criticidad = Impacto potencial * Probabilidad de ocurrencia
```

Por ejemplo, un riesgo con un impacto potencial alto y una probabilidad de ocurrencia alta tendrá una criticidad alta. Un riesgo con un impacto potencial bajo y una probabilidad de ocurrencia baja tendrá una criticidad baja.

El Concejo Municipal de Yumbo debe establecer un proceso de evaluación de riesgos que sea:

- Completo: El proceso debe considerar todos los riesgos relevantes para el Concejo Municipal de Yumbo.
- Objetivo: El proceso debe ser imparcial y no debe estar sesgado por los intereses de ninguna persona o grupo.
- Actualizado: El proceso debe ser revisado periódicamente para garantizar que sigue siendo relevante para los riesgos actuales que enfrenta el Concejo Municipal de Yumbo.

Recomendaciones para el Concejo Municipal de Yumbo

El Concejo Municipal de Yumbo puede considerar las siguientes recomendaciones para establecer un proceso de evaluación de riesgos:

- Crear un equipo de evaluación de riesgos: El equipo debe estar formado por personas con experiencia en seguridad de la información y en los riesgos específicos a los que está expuesto el Concejo Municipal de Yumbo.
- Desarrollar una metodología de evaluación de riesgos: La metodología debe ser clara y concisa, y debe ser fácil de seguir.
- Utilizar escalas objetivas para medir el impacto potencial y la probabilidad de ocurrencia de los riesgos: Las escalas deben ser establecidas por el equipo de evaluación de riesgos.
- Realizar revisiones periódicas del proceso de evaluación de riesgos: Las revisiones deben garantizar que el proceso sigue siendo relevante y eficaz.

La implementación de un proceso de evaluación de riesgos eficaz ayudará al Concejo Municipal de Yumbo a identificar los riesgos más críticos y priorizar las medidas de mitigación.

7.2. Asignación de niveles de riesgo para priorizar las medidas de mitigación

Una vez que se ha calculado la criticidad de los riesgos, se pueden asignar niveles de riesgo para priorizar las medidas de mitigación. Los niveles de riesgo se pueden asignar utilizando una escala, como la siguiente:

NIVEL DE RIESGO	CRITICIDAD
Crítico	Alta
Alto	Media
Moderado	Baja
Bajo	Muy baja

Los riesgos críticos son los que tienen una criticidad alta. Estos riesgos deben ser mitigados primero, ya que tienen el potencial de causar un impacto significativo en el Concejo Municipal de Yumbo.

Los riesgos altos son los que tienen una criticidad media. Estos riesgos también deben ser mitigados, pero pueden ser mitigados después de los riesgos críticos.

Los riesgos moderados son los que tienen una criticidad baja. Estos riesgos pueden ser mitigados posteriormente.

Los riesgos bajos son los que tienen una criticidad muy baja. Estos riesgos pueden ser mitigados, pero no son una prioridad.

La asignación de niveles de riesgo ayuda a garantizar que las medidas de mitigación se concentren en los riesgos más críticos.

Recomendaciones para el Concejo Municipal de Yumbo

El Concejo Municipal de Yumbo puede considerar las siguientes recomendaciones para asignar niveles de riesgo:

- Utilizar una escala de niveles de riesgo que sea clara y concisa: La escala debe ser fácil de entender y de aplicar.

- Asignar niveles de riesgo de forma consistente: Los niveles de riesgo deben asignarse de forma consistente a todos los riesgos, independientemente de quién los haya identificado.
- Revisar los niveles de riesgo periódicamente: Los niveles de riesgo deben revisarse periódicamente para garantizar que siguen siendo relevantes.

La implementación de un proceso de asignación de niveles de riesgo eficaz ayudará al Concejo Municipal de Yumbo a priorizar las medidas de mitigación y proteger su información.

8. MEDIDAS DE MITIGACIÓN

8.1. Desarrollo de estrategias y controles para mitigar cada riesgo identificado.

Una vez que se han identificado y evaluado los riesgos, se deben desarrollar estrategias y controles para mitigarlos. Las estrategias y controles deben ser diseñados para reducir la probabilidad de ocurrencia del riesgo o el impacto potencial del riesgo.

Estrategias de mitigación

Las estrategias de mitigación son los enfoques generales que se utilizarán para mitigar los riesgos. Las estrategias de mitigación pueden incluir:

- Evitar el riesgo: Esta estrategia consiste en eliminar la fuente del riesgo. Por ejemplo, el Concejo Municipal de Yumbo podría evitar el riesgo de robo de datos eliminando la información confidencial de los sistemas informáticos.
- Reducir la probabilidad de ocurrencia del riesgo: Esta estrategia consiste en tomar medidas para reducir la probabilidad de que ocurra el riesgo. Por ejemplo, el Concejo Municipal de Yumbo podría reducir la probabilidad de ocurrencia del robo de datos implementando controles de seguridad, como firewalls y antivirus.
- Reducir el impacto potencial del riesgo: Esta estrategia consiste en tomar medidas para reducir el impacto potencial del riesgo si ocurre. Por ejemplo, el Concejo Municipal de Yumbo podría reducir el impacto potencial del robo de datos realizando copias de seguridad de la información confidencial.

Controles de mitigación

Los controles de mitigación son las medidas específicas que se implementarán para mitigar los riesgos. Los controles de mitigación pueden ser técnicos, administrativos o de comportamiento.

- Controles técnicos: Los controles técnicos son controles que utilizan la tecnología para mitigar los riesgos. Por ejemplo, los firewalls y los antivirus son controles técnicos que se utilizan para mitigar el riesgo de robo de datos.
- Controles administrativos: Los controles administrativos son controles que no utilizan la tecnología para mitigar los riesgos. Por ejemplo, las políticas de seguridad de la información son controles administrativos que se utilizan para mitigar el riesgo de robo de datos.
- Controles de comportamiento: Los controles de comportamiento son controles que se centran en el comportamiento de las personas para mitigar los riesgos. Por ejemplo, la capacitación en seguridad de la información es un control de comportamiento que se utiliza para mitigar el riesgo de robo de datos.

Recomendaciones para el Concejo Municipal de Yumbo

El Concejo Municipal de Yumbo puede considerar las siguientes recomendaciones para desarrollar estrategias y controles de mitigación:

- Considerar los objetivos de seguridad de la información del Concejo Municipal de Yumbo: Las estrategias y controles de mitigación deben estar alineados con los objetivos de seguridad de la información del Concejo Municipal de Yumbo.
- Considerar los recursos disponibles del Concejo Municipal de Yumbo: Las estrategias y controles de mitigación deben ser factibles de implementar con los recursos disponibles del Concejo Municipal de Yumbo.
- Revisar las estrategias y controles de mitigación periódicamente: Las estrategias y controles de mitigación deben revisarse periódicamente para garantizar que siguen siendo eficaces.

La implementación de estrategias y controles de mitigación eficaces ayudará al Concejo Municipal de Yumbo a proteger su información de los riesgos.

Ejemplo de estrategia de mitigación

Para el riesgo de robo de datos, el Concejo Municipal de Yumbo podría implementar la siguiente estrategia de mitigación:

Estrategia: Reducir la probabilidad de ocurrencia del riesgo

Medidas:

- Implementar controles técnicos, como firewalls y antivirus.
- Implementar controles de acceso, como la autenticación de dos factores.
- Capacitar a los empleados sobre las amenazas de seguridad de la información.

Esta estrategia de mitigación debería ayudar a reducir la probabilidad de que ocurra el robo de datos.

8.2. Asignación de responsabilidades para la implementación de medidas específicas.

Una vez que se han desarrollado las estrategias y controles de mitigación, se deben asignar responsabilidades para la implementación de las medidas específicas. Las responsabilidades deben ser claras y concisas, y deben estar documentadas.

La asignación de responsabilidades ayuda a garantizar que las medidas de mitigación se implementen de forma eficaz y eficiente.

Recomendaciones para el Concejo Municipal de Yumbo

El Concejo Municipal de Yumbo puede considerar las siguientes recomendaciones para asignar responsabilidades para la implementación de medidas específicas:

- Considerar las habilidades y experiencia de los empleados: Las responsabilidades deben asignarse a empleados que tengan las habilidades y experiencia necesarias para implementar las medidas de mitigación.
- Proporcionar capacitación a los empleados: Los empleados deben recibir capacitación sobre las medidas de mitigación que deben implementar.

- Realizar un seguimiento del progreso: Se debe realizar un seguimiento del progreso de la implementación de las medidas de mitigación para garantizar que se cumplan los plazos y los objetivos.

La asignación de responsabilidades eficaz ayudará al Concejo Municipal de Yumbo a garantizar que las medidas de mitigación se implementen de forma correcta y oportuna.

Ejemplo de asignación de responsabilidades

Para la implementación de la estrategia de mitigación del robo de datos, el Concejo Municipal de Yumbo podría asignar las siguientes responsabilidades:

- Implementación de controles técnicos: La responsabilidad de implementar los controles técnicos, como firewalls y antivirus, podría asignarse al equipo de TI del Concejo Municipal de Yumbo.
- Implementación de controles de acceso: La responsabilidad de implementar los controles de acceso, como la autenticación de dos factores, podría asignarse al departamento de Recursos Humanos del Concejo Municipal de Yumbo.
- Capacitación a los empleados: La responsabilidad de capacitar a los empleados sobre las amenazas de seguridad de la información podría asignarse al equipo de seguridad del Concejo Municipal de Yumbo.

Esta asignación de responsabilidades debería ayudar a garantizar que las medidas de mitigación se implementen de forma eficaz y eficiente.

8.3. Integración de controles técnicos, organizativos y físicos.

Los controles de mitigación pueden ser técnicos, organizativos o físicos. Los controles técnicos utilizan la tecnología para mitigar los riesgos, los controles organizativos no utilizan la tecnología para mitigar los riesgos, y los controles físicos utilizan la seguridad física para mitigar los riesgos.

Para que las medidas de mitigación sean eficaces, es importante que se integren entre sí. La integración de los controles técnicos, organizativos y físicos ayuda a crear un enfoque holístico de la seguridad de la información.

Recomendaciones para el Concejo Municipal de Yumbo

El Concejo Municipal de Yumbo puede considerar las siguientes recomendaciones para integrar los controles técnicos, organizativos y físicos:

- Considerar los riesgos específicos a los que está expuesto el Concejo Municipal de Yumbo: La integración de los controles debe tener en cuenta los riesgos específicos a los que está expuesto el Concejo Municipal de Yumbo.
- Considerar las capacidades y limitaciones de los controles: La integración de los controles debe tener en cuenta las capacidades y limitaciones de los controles.
- Realizar pruebas de concepto: Se deben realizar pruebas de concepto para garantizar que la integración de los controles sea eficaz.

La integración eficaz de los controles técnicos, organizativos y físicos ayudará al Concejo Municipal de Yumbo a proteger su información de los riesgos.

Ejemplo de integración de controles

Para mitigar el riesgo de robo de datos, el Concejo Municipal de Yumbo podría implementar la siguiente integración de controles:

- Controles técnicos: Implementar firewalls y antivirus para bloquear el acceso no autorizado a los sistemas informáticos.
- Controles organizativos: Implementar políticas de seguridad de la información para definir las pautas de seguridad de la información.
- Controles físicos: Implementar controles de acceso físico a los sistemas informáticos para restringir el acceso a personas no autorizadas.

Esta integración de controles debería ayudar a mitigar el riesgo de robo de datos.

La identificación, evaluación y mitigación de riesgos son pasos esenciales para la gestión de la seguridad de la información. La implementación de una estrategia de mitigación eficaz ayudará al Concejo Municipal de Yumbo a proteger su información de los riesgos.

9. PLAN DE RESPUESTA A INCIDENTES:

9.1. Establecimiento de un procedimiento claro y escalonado para responder a incidentes de seguridad

Un plan de respuesta a incidentes es un documento que describe los pasos que se seguirán para responder a un incidente de seguridad de la información. El plan debe ser claro y escalonado, y debe estar documentado.

El procedimiento de respuesta a incidentes debe incluir los siguientes pasos:

- Identificación: El primer paso es identificar el incidente. Esto puede hacerse mediante la detección de señales de advertencia, como anomalías en el tráfico de red o cambios en los sistemas.

Fuente: Incibe



ILUSTRACIÓN 1. FASES DE LA RESPUESTA A INCIDENTES[1]

Pasos de identificación en un plan de respuesta a incidentes

La fase de identificación en un plan de respuesta a incidentes es la etapa en la que se detecta un incidente. Esta fase es importante para garantizar que el incidente se responda lo antes posible.

[1] https://www.incibe.es/empresas/blog/respuesta-incidentes-estais-preparados

Los pasos de identificación en un plan de respuesta a incidentes pueden variar en función de la naturaleza y el alcance del incidente. Sin embargo, algunos pasos comunes incluyen los siguientes:

- Implementar mecanismos de detección: El primer paso es implementar mecanismos de detección que puedan identificar los incidentes. Estos mecanismos pueden incluir sistemas de detección de intrusiones (IDS), sistemas de detección de malware y sistemas de monitorización del rendimiento.

  Mecanismos de detección en un plan de respuesta a incidentes

- Formar al personal: El personal debe estar formado para identificar los signos de un incidente. Esto puede incluir capacitación sobre los indicadores de compromiso (IOC), los indicadores de ataque (IOA) y los indicadores de comportamiento anormal (IBA).
- Comunicación de alertas: Las alertas deben comunicarse de manera efectiva a las partes interesadas pertinentes. Esto puede incluir la creación de procedimientos de notificación y la capacitación del personal sobre cómo responder a las alertas.

Recomendaciones para el Concejo Municipal de Yumbo

El Concejo Municipal de Yumbo puede considerar las siguientes recomendaciones para los pasos de identificación en un plan de respuesta a incidentes:

- Implementar una variedad de mecanismos de detección: El Concejo Municipal de Yumbo debe implementar una variedad de mecanismos de detección para garantizar que los incidentes se detecten de manera efectiva.
- Formar al personal de manera regular: El Concejo Municipal de Yumbo debe formar al personal de manera regular para garantizar que estén actualizados sobre los signos de un incidente.
- Probar los mecanismos de detección: El Concejo Municipal de Yumbo debe probar los mecanismos de detección periódicamente para garantizar que funcionen correctamente.

Un plan de respuesta a incidentes eficaz ayudará al Concejo Municipal de Yumbo a identificar los incidentes de seguridad de la información de manera rápida y efectiva.

Fuente: SuDigitalLawyer



ILUSTRACIÓN 2. PASOS DE INVESTIGACIÓN EN UN PLAN DE RESPUESTA A INCIDENTES[2]

Pasos de investigación en un plan de respuesta a incidentes

La fase de investigación de un plan de respuesta a incidentes es la etapa en la que se recopilan datos para determinar la naturaleza y el alcance del incidente. Esta fase es importante para tomar las medidas adecuadas para responder al incidente.

Los pasos de investigación en un plan de respuesta a incidentes pueden variar en función de la naturaleza y el alcance del incidente. Sin embargo, algunos pasos comunes incluyen los siguientes:

- Recopilación de datos: El primer paso es recopilar datos sobre el incidente. Estos datos pueden incluir registros de sistemas, registros de seguridad, información de las víctimas y testimonios de testigos.
- Análisis de datos: Una vez que se han recopilado los datos, se deben analizar para determinar la naturaleza y el alcance del incidente. Esto puede incluir el uso de herramientas forenses para analizar los datos.

[2] www.susanagonzalez.es

- Identificación de la causa: El objetivo de la investigación es identificar la causa del incidente. Esto ayudará a tomar las medidas adecuadas para evitar que vuelva a ocurrir.

Recomendaciones para el Concejo Municipal de Yumbo

El Concejo Municipal de Yumbo puede considerar las siguientes recomendaciones para los pasos de investigación en un plan de respuesta a incidentes:

- Tener un equipo de investigación: El Concejo Municipal de Yumbo debe tener un equipo de investigación capacitado para investigar los incidentes de seguridad de la información.
- Involucrar a las partes interesadas: El Concejo Municipal de Yumbo debe involucrar a las partes interesadas, como el equipo de TI, el equipo de seguridad y los empleados, en la planificación de la investigación.
- Probar el plan: El Concejo Municipal de Yumbo debe probar el plan de investigación periódicamente para garantizar que sea eficaz.

Un plan de investigación eficaz ayudará al Concejo Municipal de Yumbo a determinar la causa de los incidentes de seguridad de la información y tomar las medidas adecuadas para evitar que vuelvan a ocurrir.

Ejemplo de pasos de investigación en un plan de respuesta a incidentes

Para un incidente de malware, los pasos de investigación podrían ser los siguientes:

1. Recopilación de datos: El equipo de investigación recopilaría datos, como registros de sistemas y registros de seguridad, para determinar la naturaleza y el alcance del incidente.
2. Análisis de datos: El equipo de investigación analizaría los datos utilizando herramientas forenses para identificar el malware y su origen.
3. Identificación de la causa: El equipo de investigación determinaría cómo el malware ingresó al sistema.

Estos pasos son solo un ejemplo, y los pasos específicos que se deben seguir variarán en función de la naturaleza y el alcance del incidente.

Fuente: clima risk



ILUSTRACIÓN 3. PASOS DE CONTINUIDAD DEL NEGOCIO[3]

Pasos de continuidad del negocio en un plan de respuesta a incidentes

La fase de continuidad del negocio de un plan de respuesta a incidentes es la etapa en la que se toman medidas para garantizar que el negocio pueda continuar sus operaciones a pesar del incidente. Esta fase es importante para minimizar el impacto del incidente en las operaciones del negocio.

Los pasos de continuidad del negocio en un plan de respuesta a incidentes pueden variar en función de la naturaleza y el alcance del incidente. Sin embargo, algunos pasos comunes incluyen los siguientes:

- Identificación de los procesos críticos: El primer paso es identificar los procesos críticos del negocio que deben mantenerse operativos durante el incidente.
- Despliegue de planes de contingencia: Una vez que se han identificado los procesos críticos, se deben desplegar los planes de contingencia correspondientes. Los planes de contingencia pueden incluir la implementación de procedimientos de respaldo y recuperación, la activación de centros de operaciones de emergencia o la reubicación de empleados.
- Comunicación con las partes interesadas: Es importante comunicar con las partes interesadas, como los empleados, los clientes y los reguladores, sobre los impactos del incidente y los planes para la continuidad del negocio.

[3] Pasos de continuidad del negocio

Recomendaciones para el Concejo Municipal de Yumbo

El Concejo Municipal de Yumbo puede considerar las siguientes recomendaciones para los pasos de continuidad del negocio en un plan de respuesta a incidentes:

- Tener un plan de continuidad del negocio: El Concejo Municipal de Yumbo debe tener un plan de continuidad del negocio que describa cómo se mantendrá operativo el negocio durante un incidente.
- Involucrar a las partes interesadas: El Concejo Municipal de Yumbo debe involucrar a las partes interesadas, como el equipo de TI, el equipo de seguridad y los empleados, en la planificación de la continuidad del negocio.
- Probar el plan: El Concejo Municipal de Yumbo debe probar el plan de continuidad del negocio periódicamente para garantizar que sea eficaz.

Un plan de continuidad del negocio eficaz ayudará al Concejo Municipal de Yumbo a garantizar que el negocio pueda continuar sus operaciones a pesar de los incidentes de seguridad de la información.

Ejemplo de pasos de continuidad del negocio en un plan de respuesta a incidentes

Para un incidente de interrupción de la red, los pasos de continuidad del negocio podrían ser los siguientes:

1. Identificación de los procesos críticos: El equipo de respuesta a incidentes identificaría los procesos críticos del negocio que deben mantenerse operativos durante el incidente. Estos podrían incluir procesos como la atención al cliente, la facturación y la nómina.
2. Despliegue de planes de contingencia: El equipo de respuesta a incidentes desplegaría los planes de contingencia correspondientes. Estos podrían incluir la activación de un centro de operaciones de emergencia para coordinar las operaciones durante el incidente, o la reubicación de empleados a un sitio alternativo.
3. Comunicación con las partes interesadas: El equipo de respuesta a incidentes comunicaría con las partes interesadas, como los empleados, los clientes y los reguladores, sobre los impactos del incidente y los planes para la continuidad del negocio.

Estos pasos son solo un ejemplo, y los pasos específicos que se deben seguir variarán en función de la naturaleza y el alcance del incidente.

Fuente: Ciber Zaintza

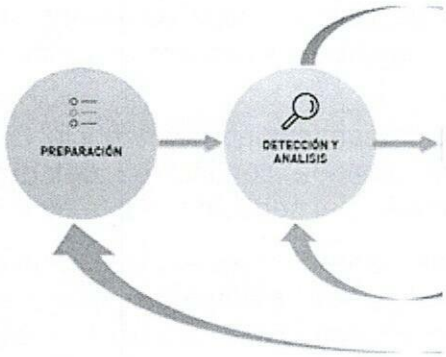


ILUSTRACIÓN 4. PASOS DEL PLAN DE RESPUESTA A INCIDENTES[4]

Pasos de respuesta en un plan de respuesta a incidentes

La fase de respuesta de un plan de respuesta a incidentes es la etapa en la que se toman medidas para detener el incidente y mitigar su impacto. Esta fase es importante para minimizar el daño y garantizar la seguridad de la información.

Los pasos de respuesta en un plan de respuesta a incidentes pueden variar en función de la naturaleza y el alcance del incidente. Sin embargo, algunos pasos comunes incluyen los siguientes:

- Evaluación del incidente: El primer paso es evaluar el incidente para determinar su naturaleza y alcance. Esto puede incluir la recopilación de datos, como registros de sistemas y registros de seguridad.
- Contención del incidente: Una vez que se ha determinado la naturaleza y el alcance del incidente, se debe tomar medidas para contenerlo. Esto puede incluir la desconexión de los sistemas afectados de la red o la eliminación de la amenaza.

[4] https://www.ciberseguridad.eus/empresa-segura/medidas-para-mitigar/plan-de-respuesta-incidentes-de-ciberseguridad

- Eliminación de la amenaza: Una vez que el incidente se ha contenido, se debe eliminar la amenaza. Esto puede incluir la eliminación de malware o la reparación de vulnerabilidades.
- Notificación a las partes interesadas: Es importante notificar a las partes interesadas del incidente, como los empleados, los clientes y los reguladores.

Recomendaciones para el Concejo Municipal de Yumbo

El Concejo Municipal de Yumbo puede considerar las siguientes recomendaciones para los pasos de respuesta en un plan de respuesta a incidentes:

- Tener un equipo de respuesta a incidentes: El Concejo Municipal de Yumbo debe tener un equipo de respuesta a incidentes entrenado y preparado para responder a incidentes de seguridad de la información.
- Involucrar a las partes interesadas: El Concejo Municipal de Yumbo debe involucrar a las partes interesadas, como el equipo de TI, el equipo de seguridad y los empleados, en la planificación de la respuesta.
- Probar el plan: El Concejo Municipal de Yumbo debe probar el plan de respuesta periódicamente para garantizar que sea eficaz.

Un plan de respuesta eficaz ayudará al Concejo Municipal de Yumbo a detener los incidentes de seguridad de la información y mitigar su impacto.

Ejemplo de pasos de respuesta en un plan de respuesta a incidentes

Para un incidente de malware, los pasos de respuesta podrían ser los siguientes:

1. Evaluación del incidente: El equipo de respuesta a incidentes recopilaría datos, como registros de sistemas y registros de seguridad, para determinar la naturaleza y el alcance del incidente.
2. Contención del incidente: El equipo de respuesta a incidentes desconectaría los sistemas afectados de la red para evitar que el malware se propague.
3. Eliminación de la amenaza: El equipo de respuesta a incidentes eliminaría el malware de los sistemas afectados.
4. Notificación a las partes interesadas: El equipo de respuesta a incidentes notificaría a los empleados, los clientes y los reguladores del incidente.

Estos pasos son solo un ejemplo, y los pasos específicos que se deben seguir variarán en función de la naturaleza y el alcance del incidente.

Pasos de recuperación en un plan de respuesta a incidentes

La fase de recuperación de un plan de respuesta a incidentes es la etapa en la que se toman medidas para restaurar los sistemas y la información afectados por el incidente. Esta fase es importante para minimizar el impacto del incidente y garantizar que el negocio pueda reanudar sus operaciones.

Los pasos de recuperación en un plan de respuesta a incidentes pueden variar en función de la naturaleza y el alcance del incidente. Sin embargo, algunos pasos comunes incluyen los siguientes:

- Restauración de los sistemas y la información: El primer paso es restaurar los sistemas y la información afectados por el incidente. Esto puede hacerse mediante la restauración de copias de seguridad o la implementación de medidas de recuperación ante desastres.
- Investigación del incidente: Es importante investigar el incidente para determinar la causa y las medidas que se pueden tomar para evitar que vuelva a ocurrir.
- Notificación a las partes interesadas: Es importante notificar a las partes interesadas del incidente, como los empleados, los clientes y los reguladores.
- Mejora de la seguridad: Es importante implementar cambios para mejorar la seguridad de la información para evitar que ocurran incidentes similares en el futuro.

Recomendaciones para el Concejo Municipal de Yumbo

El Concejo Municipal de Yumbo puede considerar las siguientes recomendaciones para los pasos de recuperación en un plan de respuesta a incidentes:

- Tener un plan de respaldo y recuperación: El Concejo Municipal de Yumbo debe tener un plan de respaldo y recuperación para restaurar los sistemas y la información afectados por un incidente.
- Involucrar a las partes interesadas: El Concejo Municipal de Yumbo debe involucrar a las partes interesadas, como el equipo de TI, el equipo de seguridad y los empleados, en la planificación de la recuperación.

- Probar el plan: El Concejo Municipal de Yumbo debe probar el plan de recuperación periódicamente para garantizar que sea eficaz.

Un plan de recuperación eficaz ayudará al Concejo Municipal de Yumbo a minimizar el impacto de los incidentes de seguridad de la información y garantizar que el negocio pueda reanudar sus operaciones.

Recomendaciones para el Concejo Municipal de Yumbo

El Concejo Municipal de Yumbo puede considerar las siguientes recomendaciones para establecer un procedimiento claro y escalonado para responder a incidentes de seguridad:

- Involucrar a todas las partes interesadas: El plan de respuesta a incidentes debe ser desarrollado con la participación de todas las partes interesadas, como el equipo de TI, el equipo de seguridad, la administración y los empleados.
- Documentar el plan: El plan de respuesta a incidentes debe estar documentado y actualizado periódicamente.
- Probar el plan: El plan de respuesta a incidentes debe probarse periódicamente para garantizar que sea eficaz.

Un plan de respuesta a incidentes eficaz ayudará al Concejo Municipal de Yumbo a responder de manera rápida y efectiva a los incidentes de seguridad de la información.

9.2. Designación de un equipo de respuesta y roles específicos.

El equipo de respuesta a incidentes (ERI) es el grupo de personas responsables de responder a los incidentes de seguridad de la información. El ERI debe estar compuesto por personas con las habilidades y conocimientos necesarios para responder a incidentes de diferentes tipos y tamaños.

Los roles específicos del ERI pueden variar en función del tamaño y la estructura de la organización. Sin embargo, algunos roles comunes incluyen los siguientes:

- Líder del equipo: El líder del equipo es responsable de la coordinación de la respuesta al incidente.

- Investigador: El investigador es responsable de recopilar datos sobre el incidente.
- Contenedor: El contenedor es responsable de contener el incidente para evitar que se propague.
- Eliminator: El eliminador es responsable de eliminar la amenaza que causó el incidente.
- Comunicador: El comunicador es responsable de comunicar el incidente a las partes interesadas.

El Concejo Municipal de Yumbo debe designar un ERI que esté compuesto por personas con las siguientes habilidades y conocimientos:

- Conocimiento de los sistemas y procesos de la organización.
- Experiencia en la respuesta a incidentes de seguridad de la información.
- Habilidades de comunicación y colaboración.

El Concejo Municipal de Yumbo debe documentar los roles y responsabilidades del ERI en el plan de respuesta a incidentes. Esto ayudará a garantizar que el ERI esté preparado para responder a los incidentes de manera efectiva.

Recomendaciones específicas para el Concejo Municipal de Yumbo

El Concejo Municipal de Yumbo puede considerar las siguientes recomendaciones para la designación de un equipo de respuesta a incidentes:

- Incluir representantes de todas las partes interesadas relevantes: El ERI debe incluir representantes de todas las partes interesadas relevantes, como el equipo de TI, el equipo de seguridad, la administración, empleados y contratistas.
- Proporcionar capacitación al ERI: El ERI debe recibir capacitación regular sobre cómo responder a incidentes de seguridad de la información.
- Probar el ERI periódicamente: El ERI debe probarse periódicamente para garantizar que esté preparado para responder a incidentes.

Un ERI eficaz ayudará al Concejo Municipal de Yumbo a responder a los incidentes de seguridad de la información de manera rápida y efectiva.

10. CONCIENTIZACIÓN Y FORMACIÓN

10.1. Fomento de la conciencia sobre la importancia de la seguridad y privacidad de la información

La concientización sobre la seguridad de la información es el proceso de educar a los empleados sobre la importancia de proteger la información de la organización. La concientización sobre la seguridad de la información es una parte importante de cualquier programa de seguridad de la información, ya que ayuda a crear una cultura de seguridad en la organización.

El Concejo Municipal de Yumbo puede fomentar la conciencia sobre la seguridad y privacidad de la información mediante una variedad de actividades, como:

- Campañas de comunicación: El Concejo Municipal de Yumbo puede crear campañas de comunicación para informar a los empleados sobre los riesgos de seguridad de la información y cómo protegerse. Las campañas de comunicación pueden utilizar una variedad de medios, como folletos, correos electrónicos, videos y eventos.

  Campaña de comunicación de seguridad de la información

- Programas de formación: El Concejo Municipal de Yumbo puede ofrecer programas de formación para los empleados sobre seguridad de la información. Los programas de formación pueden cubrir una variedad de temas, como los tipos de amenazas de seguridad de la información, las mejores prácticas de seguridad y cómo responder a un incidente de seguridad de la información.
- Incentivos: El Concejo Municipal de Yumbo puede ofrecer incentivos a los empleados que participen en actividades de concientización sobre la seguridad de la información. Los incentivos pueden incluir premios, reconocimientos o días libres.

Recomendaciones para el Concejo Municipal de Yumbo

El Concejo Municipal de Yumbo puede considerar las siguientes recomendaciones para fomentar la conciencia sobre la seguridad y privacidad de la información:

- Hacer que la concientización sobre la seguridad de la información sea un requisito: El Concejo Municipal de Yumbo puede hacer que la concientización sobre la seguridad de la información sea un requisito para todos los empleados. Esto ayudará a garantizar que todos los empleados estén informados sobre los riesgos de seguridad de la información.
- Hacer que la concientización sobre la seguridad de la información sea continua: El Concejo Municipal de Yumbo debe ofrecer programas de concientización sobre la seguridad de la información de forma continua. Esto ayudará a mantener a los empleados actualizados sobre los últimos riesgos de seguridad de la información.
- Medir el éxito: El Concejo Municipal de Yumbo debe medir el éxito de sus actividades de concientización sobre la seguridad de la información. Esto ayudará a garantizar que las actividades sean eficaces.

La concientización sobre la seguridad de la información es una parte importante de cualquier programa de seguridad de la información. Al fomentar la conciencia sobre la seguridad y privacidad de la información, el Concejo Municipal de Yumbo puede ayudar a crear una cultura de seguridad en la organización y proteger su información valiosa.

11. REVISIÓN Y MEJORA CONTINUA:

11.1. Establecimiento de un calendario para revisiones periódicas del plan.

La revisión y mejora continua es una parte importante de cualquier programa de seguridad de la información. Las revisiones periódicas del plan de tratamiento de riesgos de seguridad de la información ayudan a garantizar que el plan siga siendo eficaz y se adapte a los cambios en la organización y en el entorno de amenazas.

El Concejo Municipal de Yumbo debe establecer un calendario para revisiones periódicas del plan. Las revisiones periódicas deben realizarse al menos una vez al año, pero pueden realizarse con más frecuencia si es necesario.

Las revisiones del plan deben incluir los siguientes pasos:

- Revisión de los objetivos y metas del plan: El equipo de seguridad debe revisar los objetivos y metas del plan para asegurarse de que siguen siendo relevantes para la organización.

  Revisión de objetivos y metas del plan de seguridad de la información

- Análisis del entorno de amenazas: El equipo de seguridad debe analizar el entorno de amenazas para identificar las nuevas amenazas que pueden afectar a la organización.

  Análisis del entorno de amenazas de seguridad de la información

- Evaluación de la eficacia de las medidas de seguridad: El equipo de seguridad debe evaluar la eficacia de las medidas de seguridad implementadas para mitigar los riesgos de seguridad de la información.

  Evaluación de la eficacia de las medidas de seguridad de la información

- Recomendación de mejoras: El equipo de seguridad debe recomendar mejoras al plan para garantizar que siga siendo eficaz.

Recomendaciones para el Concejo Municipal de Yumbo

El Concejo Municipal de Yumbo puede considerar las siguientes recomendaciones para el establecimiento de un calendario para revisiones periódicas del plan:

- Involucrar a las partes interesadas: El equipo de seguridad debe involucrar a las partes interesadas, como la administración y los empleados, en el proceso de revisión del plan.
- Documentar las revisiones: El equipo de seguridad debe documentar las revisiones del plan para garantizar que se realicen de forma consistente.
- Seguir las recomendaciones: El equipo de seguridad debe seguir las recomendaciones de las revisiones del plan para garantizar que el plan siga siendo eficaz.

El establecimiento de un calendario para revisiones periódicas del plan de tratamiento de riesgos de seguridad de la información ayudará al Concejo Municipal de Yumbo a garantizar que el plan siga siendo eficaz y se adapte a los cambios en la organización y en el entorno de amenazas.

11.2. Proceso de mejora continua basado en lecciones aprendidas y cambios en el entorno de seguridad.

La mejora continua es una parte esencial de cualquier programa de seguridad de la información. La mejora continua ayuda a garantizar que el programa siga siendo eficaz y se adapte a los cambios en la organización y en el entorno de amenazas.

El Concejo Municipal de Yumbo debe establecer un proceso de mejora continua basado en lecciones aprendidas y cambios en el entorno de seguridad. Este proceso debe incluir los siguientes pasos:

- Recolección de lecciones aprendidas: El equipo de seguridad debe recopilar lecciones aprendidas de los incidentes de seguridad de la información, las evaluaciones de seguridad y las revisiones del plan.
- Análisis de cambios en el entorno de seguridad: El equipo de seguridad debe analizar los cambios en el entorno de seguridad, como la aparición de nuevas amenazas o vulnerabilidades.
- Revisión del plan de tratamiento de riesgos: El equipo de seguridad debe revisar el plan de tratamiento de riesgos de seguridad de la información para identificar oportunidades de mejora.
- Implementación de mejoras: El equipo de seguridad debe implementar las mejoras recomendadas al plan.

Recomendaciones para el Concejo Municipal de Yumbo

El Concejo Municipal de Yumbo puede considerar las siguientes recomendaciones para el establecimiento de un proceso de mejora continua basado en lecciones aprendidas y cambios en el entorno de seguridad:

- Involucrar a las partes interesadas: El equipo de seguridad debe involucrar a las partes interesadas, como la administración y los empleados, en el proceso de mejora continua.
- Documentar las mejoras: El equipo de seguridad debe documentar las mejoras realizadas al plan para garantizar que se realicen de forma consistente.

- Seguir el proceso: El equipo de seguridad debe seguir el proceso de mejora continua para garantizar que el plan siga siendo eficaz.

El establecimiento de un proceso de mejora continúa basado en lecciones aprendidas y cambios en el entorno de seguridad ayudará al Concejo Municipal de Yumbo a garantizar que el plan siga siendo eficaz y se adapte a los cambios en la organización y en el entorno de amenazas.

Ejemplos de lecciones aprendidas que pueden ser útiles para la mejora continua del plan de tratamiento de riesgos de seguridad de la información:

- La falta de concientización sobre la seguridad de la información entre los empleados fue una de las causas de un incidente de seguridad.
- Una vulnerabilidad de seguridad en el software de la organización fue explotada por un atacante.
- El plan de respuesta a incidentes no fue eficaz para contener un incidente de seguridad.

Estos ejemplos pueden ayudar al Concejo Municipal de Yumbo a identificar áreas donde se pueden realizar mejoras en el plan de tratamiento de riesgos de seguridad de la información.

12. DOCUMENTACIÓN Y REPORTES:

12.1. Establecimiento de registros y documentación detallada de las actividades seguridad y privacidad

La documentación y los registros son una parte importante de cualquier programa de seguridad de la información. La documentación ayuda a garantizar que las actividades de seguridad se realicen de forma consistente y que se puedan rastrear los resultados.

El Concejo Municipal de Yumbo debe establecer un sistema de registros y documentación que incluya los siguientes elementos:

- Plan de tratamiento de riesgos de seguridad de la información: El plan de tratamiento de riesgos de seguridad de la información debe estar

documentado de forma detallada para garantizar que se implemente de forma efectiva.

- Procedimientos de seguridad: Los procedimientos de seguridad deben estar documentados para garantizar que se sigan de forma consistente.
- Registros de seguridad: Los registros de seguridad, como los registros de incidentes, los registros de auditoría y los registros de acceso, deben conservarse para rastrear los resultados de las actividades de seguridad.

Recomendaciones para el Concejo Municipal de Yumbo

El Concejo Municipal de Yumbo puede considerar las siguientes recomendaciones para el establecimiento de un sistema de registros y documentación:

- Utilizar un modelo de documentación estándar: El Concejo Municipal de Yumbo puede utilizar un modelo de documentación estándar para garantizar que los registros y la documentación sean consistentes.
- Revisar la documentación de forma periódica: El Concejo Municipal de Yumbo debe revisar la documentación de forma periódica para garantizar que esté actualizada.
- Proteger la documentación: El Concejo Municipal de Yumbo debe proteger la documentación para evitar que sea accedida por personas no autorizadas.

El establecimiento de un sistema de registros y documentación detallado ayudará al Concejo Municipal de Yumbo a garantizar que las actividades de seguridad se realicen de forma efectiva y que se puedan rastrear los resultados.

Ejemplos de registros y documentación que pueden ser útiles para el Concejo Municipal de Yumbo:

- Registro de incidentes de seguridad: Este registro debe incluir información sobre los incidentes de seguridad, como el tipo de incidente, la fecha y hora del incidente, el impacto del incidente y las medidas tomadas para responder al incidente.
- Registro de auditoría: Este registro debe incluir información sobre las auditorías de seguridad, como los objetivos de la auditoría, los hallazgos de la auditoría y las recomendaciones de la auditoría.

- Registro de acceso: Este registro debe incluir información sobre el acceso a los sistemas y datos, como los usuarios que tienen acceso, los privilegios de acceso y el tiempo de acceso.

Estos registros y documentación pueden ayudar al Concejo Municipal de Yumbo a identificar tendencias y riesgos, a evaluar la eficacia de las medidas de seguridad y a responder a los incidentes de seguridad.

12.2. Creación de informes regulares para la dirección y las partes interesadas.

Los informes regulares son una parte importante de cualquier programa de seguridad de la información. Los informes ayudan a la dirección y a las partes interesadas a comprender el estado de la seguridad de la información en la organización y a tomar decisiones informadas sobre las medidas de seguridad.

El Concejo Municipal de Yumbo debe crear informes regulares para la dirección y las partes interesadas que incluyan los siguientes elementos:

- Resumen de los riesgos de seguridad de la información: El informe debe incluir un resumen de los riesgos de seguridad de la información que enfrenta la organización.
- Evaluación de la eficacia de las medidas de seguridad: El informe debe evaluar la eficacia de las medidas de seguridad implementadas para mitigar los riesgos de seguridad de la información.
- Recomendaciones para mejorar la seguridad de la información: El informe debe incluir recomendaciones para mejorar la seguridad de la información en la organización.

Recomendaciones para el Concejo Municipal de Yumbo

El Concejo Municipal de Yumbo puede considerar las siguientes recomendaciones para la creación de informes regulares para la dirección y las partes interesadas:

- Utilizar un formato estándar: El Concejo Municipal de Yumbo puede utilizar un formato estándar para los informes para garantizar que sean consistentes y fáciles de entender.

- Revisar los informes de forma periódica: El Concejo Municipal de Yumbo debe revisar los informes de forma periódica para garantizar que sean relevantes y precisos.
- Comunicar los informes de forma efectiva: El Concejo Municipal de Yumbo debe comunicar los informes de forma efectiva a la dirección y las partes interesadas para garantizar que sean comprendidos.

La creación de informes regulares ayudará al Concejo Municipal de Yumbo a mantener a la dirección y a las partes interesadas informadas sobre el estado de la seguridad de la información en la organización.

Ejemplos de informes que pueden ser útiles para el Concejo Municipal de Yumbo:

- Informe de estado de seguridad de la información: Este informe puede proporcionar un resumen general del estado de la seguridad de la información en la organización.
- Informe de incidentes de seguridad: Este informe puede proporcionar información sobre los incidentes de seguridad que han ocurrido en la entidad.
- Informe de auditoría de seguridad: Este informe puede proporcionar información sobre los hallazgos de las auditorías de seguridad.

Estos informes pueden ayudar a la dirección y a las partes interesadas a comprender los riesgos de seguridad de la información que enfrenta la organización, la eficacia de las medidas de seguridad implementadas y las áreas donde se pueden realizar mejoras.

13. CONCLUSIONES

El plan de privacidad y seguridad de la información es un documento esencial para cualquier organización que quiera proteger su información. Este plan debe ser desarrollado teniendo en cuenta las necesidades específicas de la organización, y debe ser revisado y actualizado periódicamente para garantizar que sigue siendo eficaz.

Los puntos clave que se deben considerar al desarrollar un plan de privacidad y seguridad de la información son los siguientes:

- Identificación de los activos de información: La primera etapa del desarrollo del plan es identificar los activos de información de la organización, incluyendo la información confidencial, sensible o crítica.
- Análisis de riesgos: Una vez que se han identificado los activos de información, es necesario realizar un análisis de riesgos para identificar los posibles riesgos a los que están expuestos.
- Mitigación de riesgos: El siguiente paso es identificar las medidas de mitigación de riesgos que se pueden implementar para reducir la probabilidad o el impacto de los riesgos identificados.
- Asignación de funciones: Las funciones y responsabilidades relacionadas con la privacidad y la seguridad de la información deben ser asignadas a los empleados adecuados.

Revisado por: • Julio Potosí	Contratista profesional Ingeniero en Sistemas	Firma:

1. INTRODUCCION

El concejo municipal de Yumbo tomando como base a la Constitución Política de Colombia en especial el artículo 15 relacionado con la protección de datos personales como un derecho de toda persona para conocer, actualizar, rectificar y/o cancelar la información y datos personales que de ella se hayan recolectado y/o se traten en bases de datos públicas o privadas .

Es de anotar que se toma como referencias la Ley 1581 del 17 de octubre de 2012, el Congreso de la República establecer las Disposiciones Generales para la Protección de Datos Personales en Colombia, igualmente reglamentada por los Decretos 1377 de 2013 y 886 de 2014 (incorporados en el Decreto único 1074 de 2015), el Concejo Municipal de Yumbo, consciente de la responsabilidad en materia de Tratamiento de Datos tiene como objeto conocer, actualizar y rectificar la información que se haya recogido en las bases de datos y archivos.

Cabe resaltar EL CONCEJO MUNICIPAL DE YUMBO, ha elaborado el presente documento POLITICA DE TRATAMIENTO DE DATOS PERSONALES y que su aplicación es de carácter obligatorio, para todas las personas naturales o jurídicas que hagan tratamiento a los datos personales registrados en las diferentes bases de datos del Concejo Municipal de Yumbo, con el fin de proporcionar los lineamientos y obligaciones legales en materia de protección de datos personales.

2. OBJETIVO

Aplicar la ley 1581 de 2012 relacionada con el medio de recolección, almacenamiento, uso, circulación, manejo y supresión de los datos personales recolectados por el Concejo Municipal de Yumbo, a través de implementación de mecanismos que garanticen la autenticidad, confidencialidad e integridad de la información.

3. ALCANCE

La implementación se aplica a las bases de datos que administra el Concejo Municipal de Yumbo –CMY-, las cuales deben ser registradas ante la Superintendencia de Industria y Comercio, cuyo período de vigencia se contará desde la fecha de la autorización y hasta el cese de las operaciones de la entidad.

Es de obligatorio cumplimiento por parte de empleados, contratistas y terceros que laboren o tengan relación directa con la entidad. Se establecen términos y condiciones para el registro de datos personales realizado en forma presencial, no presencial y/o virtual. El Concejo Municipal de Yumbo, se encarga directamente del tratamiento de los datos Personales; sin embargo, se reserva el derecho a delegar en un tercero tal tratamiento exigiendo así mismo al encargado, la atención e implementación de los lineamientos y procedimientos idóneos para la protección de los datos personales y la estricta confidencialidad de los mismos.

Estos mecanismos establecidos determinan las condiciones bajo las cuales será procesada la información; para que los titulares de los datos puedan ejercer sus derechos de conocer, actualizar, rectificar, suprimir información y revocar la autorización otorgada.

4. MARCO LEGAL

Este procedimiento tiene su marco legal en los artículos 15 y 20 de la Constitución Política, la Ley 1581 de 2012, el Decreto 1377 de 2013 y el Decreto 886 de 2014 y las demás normas que complementen o sustituyan las anteriores. Tanto la política como el procedimiento aquí determinados tienen aplicación en las Bases de Datos y/o Archivos que contienen datos personales que están debidamente registradas en la Superintendencia de Industria y Comercio que ejercen el respectivo control.

5. DEFINICIONES

Para garantizar una correcta aplicación de lo establecido en el presente documento, se determinan las siguientes definiciones algunas de ellas en concordancia de lo establecido en el artículo 3º de la Ley 1581 de 2012 así:

Autorización: consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

Aviso de privacidad: comunicación verbal, escrita o electrónica generada por el responsable, dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

Base de datos: conjunto organizado de datos personales que sean objeto de tratamiento.

Dato personal: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Dato público: es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Datos sensibles: se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y

garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Encargado del tratamiento: persona natural o jurídica en este caso el Concejo Municipal de Yumbo, que en cumplimiento de sus funciones ejecuta el tratamiento de datos personales, de acuerdo a los principios preceptuados en el artículo 4º de la Ley 1581 de 2012.

Recolección de los datos personales: la recolección de datos deberá limitarse a aquellos datos personales que son pertinentes y adecuados para la finalidad para la cual son requeridos.

Responsable del tratamiento: empleado/Colaborador del Concejo Municipal de Yumbo que decide sobre la base de datos y/o el tratamiento de datos, de acuerdo a los principios preceptuados en el artículo 4º de la Ley 1581 de 2012.

Titular: persona natural cuyos datos sean objeto de tratamiento.

Transferencia: la transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.

Transmisión: tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

Tratamiento: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

6. RESPONSABLE

Se entiende por el **encargado** del tratamiento de datos personales a:

CONCEJO MUNICIPAL DE YUMBO
NIT. 805009462
Dirección correspondencia: Calle 5 No. 4 – 40 Barrio Belalcázar
PBX: +57 (602) 669 3742
Email: contacto@concejoumbo.gov.co
URL: www.concejoyumbo.gov.co

Se debe definir el proceso responsable de dar tratamiento a las bases de datos personales y es responsabilidad del Concejo Municipal de Yumbo registrar ante las entidades correspondientes, se debe definir un responsable a fin de establecer las responsabilidades de su administración.

La entidad adquiere el compromiso de proteger la reserva, seguridad y confidencialidad de los datos personales obtenidos mediante atención al usuario, contratos, convenios y todo tipo de vínculo con los titulares, garantizándoles la posibilidad de acceder a sus datos personales en todo momento, así como la renovación, corrección, supresión y actualización de acuerdo a los principios rectores preceptuados en el artículo 4º de la Ley 1581 de 2012 que corresponde a: Principio de legalidad en materia de tratamiento de datos; Principio de finalidad; Principio de libertad; Principio de veracidad o calidad; Principio de transparencia; Principio de acceso y circulación restringida; Principio de seguridad y Principio de confidencialidad.

7. CONTENIDO

7.1. POLITICA DE PROTECCION Y TRATAMIENTO DE DATOS PERSONALES

El Concejo Municipal de Yumbo, se compromete a garantizar y proteger el derecho fundamental de Habeas Data en todas las bases de datos y/o archivos que contengan datos personales a los cuales administre y tenga acceso dentro del cumplimiento de las actividades de su misión y la normatividad, sean estos usuarios, proveedores, trabajadores, contratistas a través del cumplimiento de las siguientes actividades:

- Registrar de conformidad a la normatividad legal ante la Superintendencia de Industria y Comercio, todas las bases de datos y/o archivos que contengan datos personales, los cuales estén bajo su tratamiento, desde la autorización hasta el cese de las operaciones de la entidad.

- Se compromete a dar cumplimiento a todas las disposiciones legales vigentes y las que se desarrollen, para garantizar en especial el cumplimiento de los principios rectores del tratamiento de los datos personales.

- La actividad relacionada con tratamiento de los datos personales será informado al titular y obedecen exclusivamente a la finalidad legal para la cual está habilitada la entidad, de acuerdo a sus actividades misionales y la relación contractual o vinculante con El Concejo Municipal de Yumbo y solo para aquellas finalidades que previa y expresamente ha autorizado el titular, así como para el cumplimiento de deberes señalados en las disposiciones vigentes.

- El tratamiento de los datos sólo podrá ejercerse con el consentimiento previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización o en ausencia de mandato legal o judicial que releve el consentimiento.

- Se garantiza que la información sujeta a tratamiento es veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

- En el tratamiento de los datos se garantiza el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

- El tratamiento de los datos está sujeto a los límites que se derivan de la naturaleza de los datos personales conforme a las disposiciones legales vigentes, la Ley y la Constitución. El tratamiento sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en las normas legales y las responsabilidades contenidas en el presente documento. Los datos personales, salvo aquellos que se consideren

información pública, no estarán disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlado por la entidad, a fin de brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a las normas legales.

- La entidad pondrá a disposición como encargada del tratamiento e implementará con los responsables del tratamiento, todas las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- Todos los empleados, contratistas y otros terceros que intervengan en el tratamiento de datos personales, están obligados a garantizar la reserva y confidencialidad de la información, inclusive después de finalizada su vinculación o relación contractual, con las labores que comprende el tratamiento, pudiendo sólo ejecutar el suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en el presente documento o en los términos en que disponga la normatividad vigente.

6.2. ETAPAS PARA PROTECCION Y TRATAMIENTO DE LA INFORMACION PERSONAL

6.2.1 Recolección y Autorización. Para la recolección, el almacenamiento, el uso, la circulación y la supresión de datos personales por parte de la entidad, se requiere del consentimiento libre, previo, expreso e informado del titular de los datos. El Concejo Municipal de Yumbo en su condición de responsable del tratamiento de datos personales, ha dispuesto de los mecanismos necesarios para obtener la autorización de los titulares garantizando en todo caso que sea posible verificar el otorgamiento de dicha autorización.

6.2.2 Constancia de Autorización. La autorización se ejecutará bajo un documento físico o electrónico según los formatos Formato de Autorización de Recolección y Uso de Datos Personales – USUARIOS, el Formato de Autorización de Recolección y Uso de Datos Personales – PROVEEDORES, y Formato de Autorización de Recolección y Uso de Datos Personales – EMPLEADOS, que permite garantizar la posterior consulta física o por otro mecanismo mediante un proceso técnico o tecnológico idóneo donde se pueda constatar o verificar, que de no haber sido autorizados por el titular, los datos nunca hubieren sido capturados y almacenados.

La obtención de la autorización se debe realizar en formatos prediseños y establecidos por la entidad con el propósito que el titular podrá elegir si acepta de la entidad responsable del tratamiento de los datos que está autorizando, la forma como serán sometidos sus datos personales y la finalidad de los mismos de manera clara, expresa y previamente a la autorización de conformidad con lo que establece las disposiciones legales.

En los formatos se debe establecer el carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre datos de niñas, niños y adolescentes ante los derechos que le asisten como titular; la identificación, dirección de correspondencia o electrónica y teléfono de contacto del responsable del tratamiento.

6.2.3 Comunicación de la Autorización. Es un documento físico o electrónico tipo formato diseñado por entidad, que se encuentra a disposición del titular para el tratamiento de sus datos personales. Por intermedio de este, se le informa al titular de la existencia de unas políticas claras sobre el tratamiento de sus datos personales y la aplicación de las mismas, así como la forma de acceder a las mismas y las características del tratamiento que se pretende dar a los datos personales recabados contenido en este documento TRATAMIENTO DE DATOS PERSONALES -CONCEJO MUNICIPAL DE YUMBO.

6.2.4 Revocatoria de la Autorización. El titular de la información puede en cualquier momento solicitar a la entidad la supresión de sus datos personales y/o revocar la autorización otorgada para el tratamiento de los mismos. La solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el titular tenga un deber legal o contractual de permanecer en la base de datos.

Para los datos recolectados antes de la expedición del Decreto 1377 de 2013, se tendrá en cuenta que El Concejo Municipal de Yumbo, solicitará la autorización de los titulares para continuar con el tratamiento de sus datos personales del modo previsto en el presente procedimiento. Además, que la entidad utilizara como mecanismos eficientes de comunicación aquellos que usa en el curso ordinario de su interacción con los titulares registrados en su base de datos. El Concejo Municipal de Yumbo dispondrá al titular mecanismos gratuitos a través de email y/o formatos disponibles en los buzones PQRS instalados en las sedes de la entidad, que son de fácil acceso para presentar la solicitud de supresión de datos o la revocatoria de la autorización otorgada.

6.2.5 Finalidad del tratamiento de los datos personales. Los datos personales administrados por el Concejo Municipal de Yumbo tendrán como único fin los siguientes:

a) Para efectuar las gestiones pertinentes para el desarrollo de la función pública de la entidad en lo que tiene que ver con el cumplimiento de la función legal y constitucional del titular de la información.

b) Para contactar al usuario a través de correo electrónico para él envió de información en relación con las funciones y/o obligaciones legales derivadas de la función pública que desempeña.

c) Para contactar al titular a través de medios telefónicos, electrónicos – SMS – Email – o Chat para envió y/o confirmación de información y datos personales necesarios para la ejecución de la función constitucional y legal.

d) Para gestionar tramites de PQRS (Quejas, Reclamos, Solicitudes).

e) Para efectuar encuestas de satisfacción respecto de los servicios ofrecidos por la entidad, al envió de noticias relacionadas con campañas de socialización o mejora de los servicios e invitaciones a eventos.

f) Para procesos de selección de proveedores, adquisición y demanda de recursos e insumos para el cumplimiento de la misión de la entidad y las que le son inherentes al desarrollo de la misma.

g) Para la ejecución y el cumplimiento de los contratos que celebre la entidad para la prestación de los servicios y cumplimiento de las funciones públicas inherentes a sus competencias.

h) Para la selección y contratación de personal que demande la entidad para su funcionamiento y operación.

i) Cuando aplique para controlar, ejecutar y evidenciar el registro de actividades dentro del cumplimiento de requisitos para acceder al Sistema General de Seguridad Social Integral implementado y al Sistema de Gestión de Salud y Seguridad en el Trabajo.

j) Para dar cumplimiento a las obligaciones contraídas por la entidad con el titular de la información, con relación al pago de salarios, prestaciones sociales y demás retribuciones según lo disponga la ley.

k) Para la suscripción de convenios interadministrativos o programas institucionales directamente o en asocio con terceros.

l) Para verificar el titular a través de consulta a bases de datos públicas o centrales de riesgos.

m) Para las demás finalidades en cumplimiento de deberes legales y reportes regulatorios conforme a lo señalado en la ley.

6.2.6 Tratamiento a los Datos personales. Se establece el término de TREINTA (30) días hábiles, contados a partir de efectuada la constancia y/o autorización respectiva del tratamiento de datos personales, para que el titular de los datos contacte a el Concejo Municipal de Yumbo para solicitar la supresión o eliminación de sus datos personales, para el caso contrario la entidad continuara realizando el tratamiento de los

datos contenidos en sus bases de datos para la finalidad o finalidades indicada(s) en el presente documento para los que fueron autorizados.

La recopilación de datos de los titulares se da para efectos del cumplimiento de la misión de la entidad y desarrollo propio de las obligaciones contractuales de el Concejo Municipal de Yumbo conforme al presente documento y se realiza con aquellos titulares con quien se ha suscrito previamente acuerdos de confidencialidad, de transmisión y garantía de reserva de la información, así como acuerdos de consulta para el desarrollo de la actividad de la entidad. En tal virtud los datos personales podrán ser compartidos, trasmitidos, entregados, transferidos o divulgados a:

a) Usuarios para efectuar las gestiones necesarias en la prestación de servicios inherentes a la entidad.

b) A los colaboradores, necesarios para el cumplimiento de deberes, derechos y obligaciones derivados de los contratos de prestación de servicios, sean estos directos o contratistas y/o convenios o alianzas comerciales.

c) A proveedores o terceros para la ejecución, adquisición y demanda de recursos, insumos, bienes y servicios que haya convenido o contratado la entidad para el cumplimiento de su misión y las que le son inherentes al desarrollo de la entidad.

d) Autoridades, asociaciones gremiales, federaciones, y demás asociaciones de entidades públicas y privadas del sector legalmente establecidas en cumplimiento de deberes legales y reportes regulatorios conforme a lo señalado en la ley o convenidos expresamente con la entidad.

e) Así como quienes administren bases de datos para efectos de la prestación de las funciones constitucionales y legales, control de requisitos para acceder al Sistema General de Seguridad Social Integral y Sistema de Gestión de Salud y Seguridad en el Trabajo.

f) Las demás entidades a las cuales se autorice expresamente por la ley.

6.2.7 Seguridad en el Tratamiento. La información que conforma los registros individuales constitutivos de los bancos de datos personales, administrados por El Concejo Municipal de Yumbo, así como el resultante de las consultas que de ella hagan sus usuarios, adoptarán los mecanismos técnicos, tecnológicos, humanos, administrativos y de equipamiento que se hagan necesarios para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado o fraudulento, a través seguridades físicas en espacios específicos para el almacenamiento, archivo y conservación, asignación de usuarios con definición de seguridad y acceso, definiciones de perfiles según responsabilidades asignadas y el establecimiento de procedimientos de control documental, implementación de

plataformas y servicios virtuales idóneos a los desarrollos tecnológicos y al tratamiento ofimático y del procesamiento de información actual.

6.2.8 Veracidad o Calidad de la Información. La información contenida en los datos sujetos a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. La entidad, realizará de manera periódica o regular actividades de actualización de datos vigentes. En el caso de los datos inactivos, la entidad supone la buena fe, la veracidad y calidad de los mismos, a menos de que existan indicios expresos en contrario. Cuando así fuere, estos datos serán marcados como posiblemente incorrectos o no veraces, su eventual corrección sólo se realizará con el consentimiento de su titular.

6.2.9 Atención de PQRS sobre datos personales. Los responsables de la custodia de los activos de información a través de los colaboradores asignados como responsables de las bases de datos y/o archivos que contiene datos personales y que son tratados por la entidad, serán los responsables de atender las PQRS y consultas ante los titulares de los datos personales. Ante ellos podrán ejerces estos sus derechos a conocer, actualizar y rectificar datos mediante el correo electrónico contacto@concejoyumbo.gov.co o al número telefónico (+57)(602) 669 3742 o a través de los canales de comunicación ya definidos en el presente documento. El titular podrá solicitar la corrección o actualización de la información o manifestar cualquier incumplimiento a cualquiera de los deberes contenidos en la Ley de protección de datos personales.

6.2.10 Derechos del Titular de la información. De acuerdo con lo preceptuado en el artículo 8 de la Ley 1581 de 2012, los titulares de los datos personales tienen los siguientes derechos a saber:

a) Conocer, actualizar y rectificar o corregir sus datos personales frente a el Concejo Municipal de Yumbo que, en este caso, será responsable del tratamiento.

b) Solicitar en cualquier tiempo prueba de la autorización otorgada a el Concejo Municipal de Yumbo en su condición de responsable del tratamiento de los datos personales.

c) Ser informado por El Concejo Municipal de Yumbo previa solicitud, respecto del uso que se les han dado a los datos personales.

d) Presentar en cualquier tiempo ante la autoridad nacional competente, es decir, ante la Superintendencia de Industria y Comercio, quejas por infracciones a lo dispuesto en la ley 1581 de 2012 sobre tratamiento de datos personales, una vez agotado el correspondiente trámite de consulta o reclamo ante el responsable del tratamiento que, en este caso, es el Concejo Municipal de Yumbo.

e) Revocar la autorización y/o solicitar la supresión de sus datos cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.

f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

6.2.11 Deberes del responsable de la información: Bajo el presente documento son deberes de los responsables de la información de bases de datos personales las siguientes:

a) Adoptar mecanismos que le permitan al titular el pleno y efectivo ejercicio del derecho de hábeas data.

b) Solicitar y conservar, copia de la respectiva autorización otorgada por el titular.

c) Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten en virtud de la autorización otorgada.

d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

e) Adoptar herramientas que permitan que la información sea veraz, completa, exacta, actualizada, comprobable y comprensible.

f) Actualizar la información, atendiendo de esta forma todas las novedades respecto de los datos del titular. Adicionalmente, se deberán implementar todas las medidas necesarias para que la información se mantenga actualizada.

g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente.

h) Usar únicamente datos cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la ley 1581 de 2012.

i) Respetar las condiciones de seguridad y privacidad de la información del titular.

j) Tramitar las consultas y reclamos formulados por los titulares.

k) Informar al encargado del tratamiento cuando determinada información se encuentra en discusión por parte del titular, una vez presentada la reclamación y no haya finalizado el trámite respectivo.

l) Informar a solicitud del titular sobre el uso dado a sus datos.

m) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.

n) Cumplir los requerimientos e instrucciones que imparta la Superintendencia de Industria y Comercio sobre el tema en particular.

6.3 CONDICIONES Y MECANISMOS PARA QUE LOS TITULARES DE LOS DATOS EJERZAN SUS DERECHOS

6.3.1 Derecho a presentar reclamos

Los titulares de la información podrán ejercer sus derechos en cualquier momento y de manera gratuita, mediante solicitud escrita o por email, dirigida al responsable o encargado del tratamiento de datos personales, precisando la identificación del titular, nombres y apellidos, dirección, teléfono y correo electrónico, si este está disponible, la descripción de los hechos que dan lugar al reclamo acompañado de los documentos que acrediten la identidad y la representación del apoderado, mediante documento idóneo y los demás que se quiera hacer valer.

Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas.

Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

6.3.2 Solicitud de datos Sensibles

Se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Para el caso de datos sensibles será potestad del titular otorgar la autorización explícita para el tratamiento de dicha información. En los eventos de recepción de datos

sensibles, el Concejo Municipal de Yumbo será riguroso en mantener la seguridad y la confidencialidad de los mismos.

Se podrá hacer uso y tratamiento de los datos sensibles cuando:

a) El tratamiento sea necesario para salvaguardar el interés vital del titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, el representante legal deberá otorgar su autorización.

b) El tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, histórica, estadística o científica, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del titular y deberán adoptarse las medidas conducentes a la supresión de identidad de los titulares.

c) El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

d) De conformidad con la excepción contenida en el literal "e" del artículo 6 de la ley 1581 de 2012, el Concejo Municipal de Yumbo podrá darles tratamiento a datos personales sensibles para una finalidad histórica, estadística o científica siempre y cuando se adopten las medidas conducentes a la supresión de identidad de los titulares.

6.3.3 Solicitud de datos de Niños, Niñas y Adolescentes - NNA. Las autorizaciones de solicitud de datos personales de menores de edad serán otorgadas por los padres, representantes legales, cuidadores o quienes ejerzan la patria potestad o acudientes debidamente autorizados, mediante prueba legal (registro civil de nacimiento, escritura pública o sentencia judicial, según sea el caso); la suscripción por parte del menor de edad, representará su consentimiento sobre la autorización otorgada por los padres o sus representantes.

Será tenida en cuenta la suscripción de la autorización por parte del menor, en tanto que él deberá ser escuchado y valorado en su opinión teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

Revisado por: Julio Potosí	Contratista profesional Ingeniero en Sistemas	Firma:

Concejo Municipal De Yumbo	**FORMATO AUTORIZACIÓN DE TRATAMIENTO DE DATOS PERSONALES** **EMPLEADOS, CONTRATISTAS Y TERCEROS** **CONCEJO MUNICIPAL DE YUMBO**	**Versión: 1** **Fecha:** **18-05-2023** Página **1** de **1**

Dando cumplimiento a lo dispuesto en la Ley 1581 de 2012, "Por el cual se dictan disposiciones generales para la protección de datos personales", autorizo al Concejo Municipal de Yumbo para tratar la información obtenida relacionada con el Tratamiento de mis datos personales suministrade de forma voluntaria y con la firma de este documento manifiesto que he sido informado de lo siguiente:

1. Autorizo al Concejo Municipal de Yumbo para recolectar, usar y tratar mis datos personales y será el responsable conforme a la Política de Tratamiento de Datos Personales que la entidad haya establecido.
2. He sido informad (@) de la (s) finalidad (es) de la recolección de los datos personales, los cuales serán de carácter facultativo o voluntario responder preguntas que versen sobre Datos Sensibles o sobre menores de edad.
3. Mis derechos como titular se encuentran previstos en la Constitución y la ley, especialmente el derecho a conocer, actualizar, rectificar y suprimir mi información personal, así como el derecho a revocar el consentimiento otorgado para el tratamiento de datos personales.
4. Mis derechos pueden ser ejercidos a través de los canales dispuestos por El Concejo Municipal de Yumbo enmarcados en la Política de Tratamiento de Datos Personales.
5. Mediante la página web de la entidad (https://www.concejoyumbo.gov.co/), podré radicar cualquier tipo de requerimiento relacionado con el tratamiento de mis datos personales.
6. El Concejo Municipal de Yumbo debe garantizar la confidencialidad, seguridad y disponibilidad de mis datos y se reservará el derecho de modificar su Política de Tratamiento de Datos Personales en cualquier momento. Cambio que me será informado y publicado oportunamente en la página web.

Se firma en la ciudad de _____, el día _____ (__) de _____ 2023.

Firma: _____
Nombre: _____
Cédula: _____