POLÍTICA DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

1.1 Responsabilidades y roles

1.1.1 Designación de un responsable de seguridad de la información (RSI) y sus funciones y responsabilidades:

LA PLATAFORMA APP/WEB, designa a una persona o equipo encargado de la seguridad de la información, y define sus roles y responsabilidades. El RSI es el encargado de asegurar que se cumpla la política de seguridad de la información. Algunas de sus responsabilidades pueden incluir la evaluación y gestión de los riesgos de seguridad, el mantenimiento y actualización de la política, y la promoción de la conciencia y la formación en seguridad para los colaboradores.

1.1.2 Identificación de los roles y responsabilidades de los colaboradores en la protección de la seguridad de la información:

Todos los colaboradores de **LA PLATAFORMA APP/WEB**, deben ser conscientes de su papel en la protección de la información de la empresa. La política de seguridad identifica los roles y responsabilidades de cada empleado en relación a la seguridad de la información. Esto incluye la obligación de notificar cualquier violación de seguridad a su superior o al RSI, la adhesión a las políticas de uso aceptable y control de acceso, y la responsabilidad de proteger la información confidencial.

1.1.3 Establecimiento de un comité de seguridad de la información para supervisar y asesorar sobre la implementación de la política:

LA PLATAFORMA APP/WEB, establecerá un comité de seguridad de la información para supervisar y asesorar sobre la implementación de la política. Este comité puede estar compuesto por representantes de diferentes áreas de la empresa y es el encargado de revisar y actualizar la política, y de proporcionar retroalimentación sobre su efectividad.

1.2 Protección de datos

1.2.1 Identificación de los datos críticos que deben protegerse:

LA PLATAFORMA APP/WEB, identifica los datos críticos que deben protegerse, e incluyen información financiera, datos personales de clientes, propiedad intelectual, etc.

1.2.2 Implementación de medidas de seguridad adecuadas, como la encriptación, la segmentación de red, la monitorización de tráfico y la autenticación de usuario:

LA PLATAFORMA APP/WEB, implementa medidas de seguridad adecuadas para proteger los datos críticos. Esto puede incluir la encriptación de datos, la segmentación de la red, la monitorización del tráfico de red y la autenticación de usuario.

1.2.3 Implementación de políticas de respaldo y recuperación de desastres para asegurar que los datos puedan recuperarse en caso de una interrupción del servicio:

LA PLATAFORMA APP/WEB, considera políticas de respaldo y recuperación de desastres para asegurar que los datos puedan recuperarse en caso de una interrupción del servicio, la misma describe los procedimientos y frecuencia de las copias de seguridad, así como las medidas de recuperación que se han establecido.

1.3 Uso aceptable

1.3.1 Pautas de uso aceptable:

LA PLATAFORMA APP/WEB, establece pautas y directrices para el uso aceptable de la política de seguridad de la información. Esto puede Incluir la prohibición de acciones no autorizadas, como el acceso no autorizado a sistemas o datos, la divulgación no autorizada de información confidencial, el uso indebido de los recursos de tecnología de la información y la violación de derechos de propiedad intelectual.

1.3.2 Comunicación de la política de uso aceptable:

LA PLATAFORMA APP/WEB, comunica y difunde de manera efectiva la política de seguridad de la información a todos los colaboradores y, cuando corresponda, a los contratistas y proveedores. Esto se realiza a través de reuniones de capacitación, manuales de procedimientos, políticas escritas, instructivos, intranets corporativas u otros medios de comunicación interna.

1.3.3 Consentimiento del personal:

Para garantizar la comprensión y el cumplimiento de la política de uso aceptable, **LA PLATAFORMA APP/WEB** puede requerir que todos los colaboradores firmen un documento de consentimiento en el que indiquen que han leído, entendido y aceptado cumplir con la política, con el fin de reforzar la importancia de la seguridad de la información y las consecuencias de su mal uso.

1.3.4 Consecuencias por incumplimiento:

La política de uso aceptable estable las consecuencias por el incumplimiento de las pautas establecidas, lo cual incluye medidas disciplinarias, como advertencias verbales o escritas, suspensiones temporales, despidos y, en casos más graves, acciones legales. Es importante puntualizar que las consecuencias son proporcionales a la gravedad del incumplimiento y se apliquen de manera consistente.

1.3.5 Monitoreo y auditorías:

LA PLATAFORMA APP/WEB, implementa mecanismos de monitoreo y auditoría para garantizar el cumplimiento de la política de uso aceptable. Esto puede incluir la supervisión de actividades en línea, la revisión de registros de acceso, la realización de pruebas de seguridad y auditorías regulares.

Estas actividades coadyuvan a identificar posibles violaciones o comportamientos de riesgo y permitirán tomar medidas correctivas oportunas.

1.3.6 Capacitación y concientización:

LA PLATAFORMA APP/WEB, proporciona capacitación regular sobre la política de uso aceptable y la importancia de la seguridad de la información. Esto puede incluir programas de capacitación en línea, seminarios presenciales, sesiones informativas o materiales educativos. Además, promociona una cultura de conciencia de seguridad en la que todos los colaboradores están comprometidos en proteger la información y reportar cualquier actividad sospechosa.

1.4 Control de acceso

1.4.1 Identificación de los diferentes niveles de acceso a los recursos y sistemas de la compañía:

LA PLATAFORMA APP/WEB, identifica los diferentes niveles de acceso a los recursos y sistemas de la empresa y quién tiene acceso a cada uno de ellos.

1.4.2 Medidas de control de acceso, como contraseñas seguras, autenticación de dos factores y la revocación de permisos de acceso:

LA PLATAFORMA APP/WEB, implementa medidas de control de acceso adecuadas para garantizar que solo se conceda acceso a los recursos y sistemas a aquellos que tienen permiso. Esto puede incluir contraseñas seguras, autenticación de dos factores y la revocación de permisos de acceso.

1.5 Comunicación y formación en seguridad

1.5.1 Política de comunicación y formación en seguridad para los colaboradores:

LA PLATAFORMA APP/WEB, considera una política de comunicación y formación en seguridad para sus empleados. Esto puede incluir la organización de sesiones de formación en seguridad, la comunicación regular sobre las amenazas de seguridad y las actualizaciones de la política de seguridad, y la realización de pruebas de conciencia en seguridad.

1.5.2 Identificación de los recursos de formación en seguridad que se ofrecen a los colaboradores:

Los recursos de formación en seguridad que se ofrecen a los colaboradores, son material de formación en línea, sesiones de formación presencial y pruebas de conciencia en seguridad.

1.6 Evaluación y gestión de riesgos

1.6.1 Evaluación y gestión de riesgos de seguridad:

LA PLATAFORMA APP/WEB, considera un proceso para la evaluación y gestión de riesgos de seguridad, el cual incluye la identificación de los riesgos potenciales, la evaluación del impacto de cada riesgo y la determinación de medidas de mitigación para reducir el riesgo.

1.6.2 Medidas de mitigación de riesgos identificados en la evaluación de riesgos:

LA PLATAFORMA APP/WEB, a través de sus procesos de seguridad industrial implementa las medidas de mitigación de riesgos identificados en la evaluación de riesgos. Esto incluye la implementación de controles de seguridad adicionales o la actualización de los procedimientos existentes.

1.6.3 Revisión y actualización periódica de la política de seguridad:

La política de seguridad es revisada y actualizada periódicamente para asegurarse de que sigue siendo relevante y efectiva, la revisión y actualización, así como las notificaciones de los cambios a los colaboradores serán realizados mediante boletines internos, en los cuales serán asegurados su comprensión y cumplimiento de los nuevos requisitos. El comité de seguridad de la información es el encargado de revisar y proponer cambios a la política, la realización de evaluaciones de riesgos periódicas para identificar nuevas amenazas y vulnerabilidades, y la consulta con expertos internos o externos en seguridad de la información.

POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

2.1 Objetivos y alcance

2.1.1 Descripción de los objetivos de la política de tratamiento de datos personales:

LA PLATAFORMA APP/WEB, ha definido los objetivos de la política de tratamiento de datos personales, los cuales incluyen la protección de la privacidad de los individuos, el cumplimiento de las leyes y regulaciones aplicables, la gestión adecuada de los datos y la confianza de los clientes en la compañía.

2.1.2 Alcance de la política:

LA PLATAFORMA APP/WEB, ha definido el alcance de la política de tratamiento de datos personales, es decir, los tipos de datos personales que la compañía recolecta, cómo los utiliza y quién tiene acceso a ellos. Esto incluye todos los procesos de la empresa en los que se manejan datos personales, como la recolección de información de los clientes, la gestión de la nómina de colaboradores y la recolección de información de los proveedores.

2.2 Responsabilidades

2.2.1 Responsable de protección de datos (DPO):

LA PLATAFORMA APP/WEB, ha designado a un DPO que supervise la implementación de la política de tratamiento de datos personales y garantice el cumplimiento de las leyes y regulaciones aplicables. El DPO tiene conocimientos técnicos y legales suficientes y estar disponible para responder a las preguntas y preocupaciones de los empleados y clientes sobre la gestión de los datos personales.

2.2.2 Identificación de las responsabilidades de la compañía:

Las responsabilidades de **LA PLATAFORMA APP/WEB**, en relación con el tratamiento de los datos personales, incluyen la recolección, uso, almacenamiento y eliminación de los datos. Adicionalmente incluyen medidas para garantizar la calidad y exactitud de los datos recolectados, así como procedimientos para garantizar la seguridad de los datos y el cumplimiento de las leyes y regulaciones aplicables.

2.2.3 Identificación de las responsabilidades de los colaboradores:

Las responsabilidades de los colaboradores en relación con el tratamiento de los datos personales, incluyen la protección de la privacidad de los individuos y la notificación de posibles violaciones de seguridad, de igual forma se considera la capacitación de los empleados en las mejores prácticas de privacidad de datos y la designación de un punto de contacto interno para la gestión de las preocupaciones y preguntas de los colaboradores sobre la política de tratamiento de datos personales.

2.3 Consentimiento y transparencia

2.3.1 Consentimiento informado:

- Establecer políticas y procedimientos claros para obtener el consentimiento informado de los individuos cuyos datos personales serán procesados.
- Informar a los individuos sobre qué datos se recopilan, cómo se utilizarán, quién los tendrá acceso y cualquier otra información relevante antes de solicitar su consentimiento.
- Obtener un consentimiento explícito y verificable, preferiblemente por escrito o mediante una acción afirmativa clara por parte del individuo.

2.3.2 Mantenimiento de registros de consentimiento:

- Mantener un registro actualizado de los consentimientos obtenidos, incluyendo la fecha, el propósito del procesamiento, el alcance del consentimiento y cualquier información adicional requerida.
- Proporcionar una forma sencilla y accesible para que los individuos puedan revocar su consentimiento en cualquier momento, y garantizar que se procesen las solicitudes de revocación de manera oportuna.

2.3.3 Transparencia en el procesamiento de datos:

- Proporcionar información clara y fácilmente comprensible sobre las prácticas de procesamiento de datos personales de la compañía.
- Elaborar una política de privacidad que describa cómo se recopilan, utilizan, almacenan y protegen los datos personales, así como los derechos de los individuos en relación con sus datos.
- Asegurarse de que la política de privacidad esté fácilmente disponible en el sitio web de la compañía y sea accesible para los individuos antes de proporcionar sus datos.

2.3.4 Notificación de brechas de seguridad:

- Establecer un proceso para detectar, evaluar y notificar las brechas de seguridad que puedan comprometer la confidencialidad o integridad de los datos personales.
- Notificar de manera oportuna a las autoridades competentes y a los individuos afectados por la brecha de seguridad, proporcionando información clara sobre el alcance de la violación y las medidas que se están tomando para remediarla.

2.3.5 Gestión de solicitudes de los individuos:

- Establecer un proceso eficiente para manejar las solicitudes de los individuos en relación con sus derechos de protección de datos, como el acceso, rectificación, eliminación o portabilidad de sus datos personales.
- Responder a estas solicitudes dentro de los plazos establecidos por la ley y garantizar que se tomen las medidas necesarias para cumplir con los derechos de los individuos.

2.4 Transferencias internacionales de datos

2.4.1 Identificación de transferencias internacionales de datos:

LA PLATAFORMA APP/WEB, identifica las transferencias internacionales de datos personales y establecer medidas para garantizar que se realicen de acuerdo con las leyes y regulaciones aplicables.

2.4.2 Garantía de la protección adecuada de los datos personales:

LA PLATAFORMA APP/WEB, establece medidas para garantizar que las transferencias internacionales de datos personales se realicen de forma segura y que se garantice la protección adecuada de los datos personales durante el proceso de transferencia. 3.5 Conservación y eliminación de datos

2.5.1 Plazos de conservación de los datos personales:

LA PLATAFORMA APP/WEB, establece plazos de conservación de los datos personales que la empresa recolecta y utiliza. Estos plazos son coherentes con las leyes y regulaciones aplicables y son revisados regularmente para garantizar que los datos personales no se retengan durante más tiempo del necesario.

2.5.2 Procedimientos para la eliminación de datos personales:

LA PLATAFORMA APP/WEB, establece procedimientos para la eliminación de los datos personales que la empresa recolecta y utiliza. Esto puede incluir la eliminación de los datos cuando ya no sean necesarios para los fines establecidos en la política de tratamiento de datos personales o cuando los individuos soliciten que se eliminen sus datos. La eliminación se realiza de manera segura y con medidas de seguridad apropiadas para garantizar que los datos personales no se puedan recuperar.