promotick

Política de Seguridad de Información

Aprobado por la Gerencia General

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Introducción

La Política de Seguridad de la Información (en adelante, Política) tiene como objetivo la adopción de un conjunto de lineamientos destinados a preservar la confidencialidad, integridad y disponibilidad de la información, que constituyen los tres componentes básicos de la seguridad de la información, y tiene como objetivo establecer los requisitos para proteger la información, los equipos y servicios tecnológicos que sirven de soporte para la mayoría de los procesos de negocio de Promotick S.A.C. (en adelante, Promotick).

Esta Política de Seguridad de la Información es la base sobre la cual se dirige el Cuerpo Normativo de Seguridad de Promotick. El Cuerpo Normativo de Seguridad (en adelante, CNS) es un conjunto de documentos a diferentes niveles que conforman los requerimientos, directrices y protocolos que debe seguir Promotick en materia de seguridad. El CNS deberá ser desarrollado Promotick mediante un conjunto de documentos (normas de uso, estándares normativos, procedimientos, manuales, guías, buenas prácticas, etc.) de tal manera que cubran todos los aspectos que se presentan en la Política, llegando a nivel de proceso operativo.

En la actualidad, las tecnologías de la información se enfrentan a un creciente número de amenazas, lo cual requiere de un esfuerzo constante por adaptarse y gestionar los riesgos introducidos por estas.

1.1. Objetivo

El objetivo principal de la presente Política de alto nivel es definir los principios y las reglas básicas para la gestión de la seguridad de la información. El fin último es lograr que Promotick garantice la seguridad de la información y minimicen los riesgos de naturaleza no financiera derivados de un impacto provocado por una gestión ineficaz de la misma.

1.2. Alcance

La Política es aplicable para todo Promotick, que deberá cumplir este mínimo requisito sin perjuicio de tener políticas más restrictivas y mejorar la seguridad en la medida de lo posible. La empresa deberá adaptar y desarrollar esta Política y deberá reportar a la matriz de su adecuación a dicha Política, en ejecución de los procesos de monitorización del sistema de gestión de cumplimiento de Promotick. El alcance de la presente Política aplica a Promotick el medio que la contenga o el lugar en el que se encuentre, ya se trate de información impresa o almacenada electrónicamente.

PROHIBIDA SU REPRODUCCIÓN

Las políticas deben ser anexadas al contrato de trabajo de todos los empleados y debe ser notificada en caso los documentos tengan alguna actualización aprobada.

Las políticas deben estar disponibles de forma permanente dentro de la página web Promotick a través del enlace https://www.promotick.com/compliance/politicasseguridad.pdf

2. Principios de la Política de la Información

La presente Política responde a las recomendaciones de las mejores prácticas de Seguridad de la Información recogidas en el Estándar Internacional ISO/IEC 27001, así como al cumplimiento de la legislación vigente en materia de protección de datos personales y de las normativas que, en el ámbito de la Seguridad de la Información, puedan afectar a Promotick.

Además, Promotick establece los siguientes principios básicos como directrices fundamentales de seguridad de la información que han de tenerse siempre presentes en cualquier actividad relacionada con el tratamiento de información:

- Alcance estratégico: La seguridad de la información deberá contar con el compromiso y apoyo de todos los niveles directivos de Promotick de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas para conformar un marco de trabajo completamente coherente y eficaz.
- Seguridad integral: La seguridad de la información se entenderá como un proceso integral constituido por elementos técnicos, humanos, materiales y organizativos, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información deberá considerarse como parte de la operativa habitual, estando presente y aplicándose durante todo el proceso de diseño, desarrollo y mantenimiento de los sistemas de información
- Gestión de riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad de la información. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que están expuestos y la eficacia y el coste de las medidas de seguridad.
- Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado.

PROHIBIDA SU REPRODUCCIÓN

- Seguridad por defecto: Los sistemas deberán diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

Promotick considera que las funciones de Seguridad de la Información deberán quedar integradas en todos los niveles jerárquicos de su personal.

Puesto que la Seguridad de la Información incumbe a todo el personal de Promotick, esta Política deberá ser conocida, comprendida y asumida por todos sus empleados.

Para la consecución de los objetivos de esta Política, Promotick deberá establecer una estrategia preventiva de análisis sobre los riesgos que pudieran afectarle, identificándolos, implantando controles para su mitigación y estableciendo procedimientos regulares para su reevaluación. En el transcurso de este ciclo de mejora continua, Promotick mantendrá la definición tanto del nivel de riesgo residual aceptado (apetito al riesgo) como de sus umbrales de tolerancia.

3. Compromiso de la Dirección

La Dirección de Promotick, consciente de la importancia de la seguridad de la información para llevar a cabo con éxito sus objetivos de negocio, se compromete a:

- Promover en la organización las funciones y responsabilidades en el ámbito de seguridad de la información.
- Facilitar los recursos adecuados para alcanzar los objetivos de seguridad de la información.
- Impulsar la divulgación y la concienciación de la Política de Seguridad de la Información entre los empleados de Promotick.
- Exigir el cumplimiento de la Política, de la legislación vigente y de los requisitos de los reguladores en el ámbito de la seguridad de la información.
- Considerar los riesgos de seguridad de la información en la toma de decisiones.

4. Roles y responsabilidades

Promotick se compromete a velar por la Seguridad de todos los activos bajo su responsabilidad mediante las medidas que sean necesarias, siempre garantizando el cumplimiento de las distintas normativas y leyes aplicables.

Promotick, deberá nombrar una figura responsable de definir, implementar y monitorizar las medidas de ciberseguridad y seguridad de la información. Esta figura deberá establecerse desde un entorno de gobierno y gestión, será independiente de cualquier área organizativa reportando al órgano de gobierno o en su defecto a su comisión de auditoría y tendrá entre sus funciones y responsabilidades el aplicar principios de segregación de funciones y el contacto con las autoridades y grupos de interés especiales en materia de seguridad de la información.

PROHIBIDA SU REPRODUCCIÓN

La figura asumirá las funciones que, con carácter general, sean atribuidas por la presente Política de Seguridad de la Información a dicha figura.

Será su responsabilidad desarrollar y mantener la Política, asegurándose que ésta sea adecuada y oportuna según evolucione la regulación vigente.

5. Gestión de la Seguridad de los Recursos Humanos

El departamento de Recursos Humanos deberá realizar su gestión teniendo en cuenta los criterios de seguridad establecidos en la Política de Seguridad de la Información, siendo este un punto clave para asegurar su cumplimiento.

Se deberán salvaguardar los requisitos establecidos en la presente Política en todo momento, incluyendo en la fase previa a la contratación, fase de contratación, y fase de desistimiento de contratos de los empleados.

5.1. Formación y concienciación

Promotick deberá asegurar que todo el personal recibe un nivel de formación y concienciación adecuado en materia de Seguridad de la Información en los plazos que exija la normativa vigente, especialmente en materia de confidencialidad y prevención de fugas de información.

Asimismo, los empleados deberán ser informados de las actualizaciones de las políticas y procedimientos de seguridad en los que se vean afectados y de las amenazas existentes, de manera que pueda garantizarse el cumplimiento de esta Política.

Por otro lado, los empleados tienen la obligación de obrar con diligencia con respecto a la información, debiéndose asegurar que dicha información no caiga en poder de empleados o terceros no autorizados.

5.2. Política de mesas limpias

Se establecen los siguientes requisitos con el objetivo de mantener la seguridad en los puestos de trabajo:

- Se deberá bloquear la sesión de los equipos cuando el empleado deje el puesto, tanto por medios manuales (bloqueo por parte del usuario), como de forma automatizada mediante la configuración del bloqueo de pantalla.
- Se deberá dejar recogido el entorno de trabajo al finalizar la jornada. Esto incluye la necesidad de que todo documento o soporte de información quede fuera de la vista, guardando bajo llave los que por su clasificación sean confidenciales o secretos (véase el Anexo: Niveles de clasificación).
- Se deberá mantener ordenado el puesto de trabajo y despejado de documentos o soportes de información que puedan ser vistos o accesibles por otras personas.

PROHIBIDA SU REPRODUCCION

6. Gestión de activos

Se deberán tener identificados e inventariados los activos de información necesarios para la prestación de los procesos de negocio de Promotick. Adicionalmente, se deberá mantener actualizado el inventario de activos.

Se deberá realizar la clasificación de los activos en función del tipo de información que se vaya a tratar, de acuerdo con lo dispuesto en el apartado *7. Clasificación de la información*.

Se deberá asignar un responsable encargado de realizar la gestión propia de los activos de información durante todo el ciclo de vida. El responsable deberá mantener un registro formal de los usuarios con acceso autorizado a dicho activo.

Además, para cada activo o elemento de información deberá existir un responsable o propietario, el cual tendrá la responsabilidad de asegurar que el activo esté inventariado, correctamente clasificado y adecuadamente protegido.

Se deberán actualizar de manera periódica las configuraciones de los activos para permitir el seguimiento de estos y facilitar una correcta actualización de la información.

6.1. Gestión del ciclo de vida de la información

Promotick deberá gestionar adecuadamente el ciclo de vida de la información, de manera que se puedan evitar usos incorrectos durante cualquiera de las fases.

El ciclo de vida de un activo de información consta de las siguientes fases:

1. Creación o recolección: esta fase se ocupa de los registros en su punto de origen. Esto podría incluir su creación por un miembro de Promotick o la recepción de información desde una fuente externa. Incluye correspondencia, formularios, informes, dibujos, entrada/salida del ordenador u otras fuentes.
2. Distribución: es el proceso de gestión de la información una vez que se ha creado o recibido. Esto incluye tanto la distribución interna como externa, ya que la información que sale de Promotick se convierte en un registro de una transacción con terceros.
3. Uso o acceso: se lleva a cabo después de que la información se distribuya internamente, y puede generar decisiones de negocio, generar nueva información, o servir para otros fines. Detalla el conjunto de usuarios autorizados por Promotick a acceder a la información.
4. Almacenamiento: es el proceso de organizar la información en una secuencia predeterminada y la creación de un sistema de gestión para garantizar su utilidad dentro de Promotick. Si no se establece un método de almacenamiento para la presentación de información, su recuperación y uso resultaría casi imposible.
5. Destrucción: establece las prácticas para la eliminación de la información que ha cumplido los periodos de retención definidos y la información que ha dejado de ser útil para Promotick. Los periodos de conservación de la información deberán

PROHIBIDA SU REPRODUCCION

estar basados en los requisitos normativos, legales y jurídicos que afectan Promotick. También deberán tenerse en cuenta las necesidades de negocio. Si ninguno de estos requisitos exige que la información sea conservada, deberá ser desechada mediante medios que garanticen su confidencialidad durante el proceso de destrucción.

Promotick deberá identificar medidas de seguridad de acuerdo con la presente Política para asegurar la correcta gestión del ciclo de vida de los activos.

6.2. Gestión de las copias de seguridad

Se deberán realizar copias de seguridad de la información, del software y del sistema y se deberán verificar periódicamente. Para ello, se deberán realizar copias de seguridad de aplicaciones, ficheros, logs del sistema y bases de datos con una periodicidad, al menos, semanal, salvo que en dicho período no se hubiese producido ninguna actualización. En su caso, se podrá establecer una frecuencia más alta de realización de copias de seguridad, si la información a salvaguardar es de impacto alto para Promotick y/o de elevado nivel de transaccionalidad.

Como normal general, la frecuencia con la que se realizarán las copias de seguridad se determinará en función de la sensibilidad de las aplicaciones o datos, de acuerdo con los criterios de clasificación de información declarados en el anexo “Niveles de clasificación”.

Las copias de seguridad deberán recibir las mismas protecciones de seguridad que los datos originales, asegurándose su correcta conservación, así como los controles de acceso adecuados.

Como norma general y siempre que sea posible, se deberá requerir que la información en las copias de seguridad esté cifrada. Este requerimiento será obligatorio para determinados tipos de información confidencial.

Se deberán realizar pruebas de restauración de las copias de seguridad disponibles y de los procesos de restauración definidos, a fin de garantizar el funcionamiento correcto de los procesos. Estas se realizarán de forma periódica y quedarán documentadas.

Se deberá establecer un período de retención de las copias de seguridad hasta su destrucción una vez terminado el periodo de existencia.

Las copias de seguridad, tanto de archivos maestros como de aplicaciones y archivos de información se deberán ubicar en lugares seguros con acceso restringido. Asimismo, las copias de respaldo se ubicarán preferentemente en un centro distinto al que las generó.

Se deberá garantizar que existe una copia de seguridad adicional de la información sensible protegida ante escritura, de forma que se garantice su integridad ante la necesidad de recuperación frente a posibles incidencias de seguridad asociadas, por ejemplo, a Ransomware.

PROHIBIDA SU REPRODUCCIÓN

7. Clasificación de la información

Se deberá definir un modelo de clasificación de la información que permita conocer e implantar las medidas técnicas y organizativas necesarias para mantener su disponibilidad, confidencialidad e integridad. El modelo de clasificación deberá integrar los requisitos y condiciones establecidos en el presente apartado de la Política.

El modelo de clasificación deberá tener un responsable encargado de su actualización cuando se crea conveniente, así como de dar a conocer el modelo de clasificación a todos los empleados de Promotick.

7.1. Tipos de información

Promotick deberá clasificar la información en función del soporte en el que está siendo utilizado:

a) Soportes lógicos: información que esté siendo utilizada mediante medios ofimáticos, correo electrónico o sistemas de información desarrollados a medida o adquiridos a un tercero.
b) Soportes físicos: información que esté en papel, soportes magnéticos como USBs, DVDs, etcétera.

7.2. Niveles de clasificación

En función de la sensibilidad de la información, Promotick deberá catalogar la información en cinco niveles, véase la definición precisa en el Anexo “Niveles de clasificación”:

- Uso público
- Difusión limitada
- Información confidencial
- Información reservada
- Información secreta

7.3. Gestión de información privilegiada

La información que se considere reservada, confidencial o secreta se deberá tratar con especial cuidado. Se deberán definir medidas de seguridad extraordinarias o adicionales para el adecuado tratado de la información privilegiada. Este tipo de información se deberá enviar cifrada y mediante protocolos seguros.

7.4. Etiquetado de la información

Promotick deberá etiquetar mediante métodos manuales o, en la medida de lo posible, automatizados para facilitar el procesamiento adecuado de las medidas de seguridad que apliquen en cada caso.

PROHIBIDA SU REPRODUCCIÓN

Se deberán etiquetar los documentos o materiales, así como los anexos, copias, traducciones o extractos de estos, según los niveles de clasificación de la información definidos en el subapartado anterior, exceptuando la información considerada de “Uso público”.

Se deberá definir un proceso o procedimiento para el etiquetado de la información de acuerdo con los siguientes requisitos:

- Asegurar que el etiquetado de la información refleja el esquema de clasificación de la información adoptado.
- Asegurar que las etiquetas sean fácilmente reconocibles entre todos los empleados.
- Orientar a los empleados sobre dónde y cómo se colocarán o utilizarán las etiquetas, en función del proceso de acceso a la información o a los activos que la soportan.
- Indicar las excepciones en los que se permite omitir el etiquetado, sin que ello suponga una omisión del deber de clasificar la información.

Se deberá prestar especial atención y tratar con cuidado máximo el etiquetado de activos físicos que contengan información reservada o secreta, para evitar su sustracción por ser fácilmente identificable.

Se deberán establecer las medidas técnicas, si fueran necesarias, y viables de etiquetado automático de la información soportada en medios digitales.

Promotick deberá asegurar la formación y capacitación de todos sus empleados en el etiquetado de la información, así como formar y capacitar específicamente a los empleados que traten información de nivel reservada o secreta.

7.5. Manipulación de la información

Promotick se encargará de desarrollar e implementar un conjunto adecuado de procedimientos para la correcta manipulación de la información. Se deberán adoptar las medidas necesarias para proteger la información de acuerdo con su clasificación.

La información privilegiada estará en todo momento custodiada durante todo el ciclo de vida de la misma.

7.6. Privacidad de la información

Promotick deberá asegurar la privacidad de los datos de carácter personal con el objetivo de proteger los derechos fundamentales de las personas físicas, especialmente su derecho al honor, intimidad personal y familiar y a la propia imagen, mediante el establecimiento de medidas para regular el tratamiento de los datos.

Promotick deberá cumplir con la legislación vigente en materia de protección de datos personales en función de la jurisdicción en la que esté establecida y opere (a modo

PROHIBIDA SU REPRODUCCION

ilustrativo, la Ley de Protección de Datos N° 29733 de la constitución política del Perú y deberá incluir las medidas necesarias para cumplir con la normativa.

Se deberán implementar medidas adecuadas para asegurar la privacidad de la información en todas las fases de su ciclo de vida (de acuerdo con el apartado *6.2. Gestión del ciclo de vida de la información*).

8. Prevención de fugas de información

La fuga de información es una salida no controlada de información (intencionada o no intencionada) que provoca que la misma llegue a personas no autorizadas o que su propietario pierda el control sobre el acceso a la misma por parte de terceros.

Se deberán analizar los vectores de fuga de información, en función de las condiciones y operativa de trabajo de Promotick. Para ello, se deberán identificar los activos cuya fuga supone mayor riesgo para la empresa, basándose en la criticidad del activo y el nivel de clasificación que la información tenga. Además, se deberán identificar las posibles vías de robo, pérdida o fuga de cada uno de los activos en sus diferentes estados del ciclo de vida.

Promotick deberá definir procedimientos para evitar la ocurrencia de las situaciones que puedan provocar la pérdida de información, así como procedimientos de actuación en caso de que se notifique una fuga de información.

Se deberá asegurar la formación y capacitación de todos los empleados en torno a buenas prácticas para la prevención de fugas de información. Especialmente se deberán tener en cuenta, al menos, los siguientes aspectos:

- Proceso para el manejo de dispositivos de alta criticidad conocidos
- Uso adecuado de dispositivos extraíbles como USBs, CD/DVDs o similares
- Uso del correo electrónico
- Transmisión de información de forma oral
- Impresión de documentación
- Salida de documentación
- Uso de dispositivos móviles
- Uso de Internet
- Escritorios limpios y ordenados (véase el apartado *5.2. Política de mesas limpias*) • Equipos desatendidos

9. Control de acceso

Todos los sistemas de información de Promotick deberán contar con un sistema de control de acceso a los mismos. Asimismo, el control de acceso se enfoca en asegurar

PROHIBIDA SU REPRODUCCIÓN

el acceso de los usuarios y prevenir el acceso no autorizado a los sistemas de información, incluyendo medidas como la protección mediante contraseñas.

El control de acceso se entenderá desde la perspectiva tanto lógica (enfocado a sistemas de la información) como física (véase el apartado *11. Seguridad Física y del Entorno*).

9.1. Requisitos de negocio para el control de acceso

Promotick deberá asumir una serie de requisitos de negocio para el control de acceso, que serán, al menos, los siguientes:

- Los usuarios deberán ser únicos y no podrán ser compartidos. Asimismo, los privilegios de los usuarios serán inicialmente asignados mediante el principio de mínimo privilegio.
- Se prohibirá el uso de usuarios genéricos. En su defecto, se utilizarán cuentas de usuario asociadas a la identidad nominal de la persona asociada.
- Siempre que sea posible, se deberá de disponer de un doble factor de autenticación (MFA) para el acceso a los sistemas de información, siendo obligatorio para aquellos que puedan ser accesibles desde redes públicas.

9.2. Derechos de acceso

Promotick deberá implementar controles de acceso que garanticen que a los usuarios sólo se les otorguen privilegios y derechos necesarios para desempeñar su función.

Los derechos de acceso deberán ser establecidos en función de:

- Control de acceso basado en roles: deberán establecerse perfiles o roles de acceso por aplicación y/o sistemas para poder asignar los mismos a los diferentes usuarios.
- Necesidad de saber: Solo se permitirá el acceso a un recurso cuando exista una necesidad legítima para el desarrollo de la actividad.
- Privilegios mínimos: los permisos otorgados a los usuarios deberán ser los mínimos.
- Segregación de funciones: deberá asegurarse una correcta segregación de funciones para desarrollar y asignar derechos de acceso.

Asimismo, ningún usuario deberá poder acceder por sí mismo a un sistema de información controlado sin la aprobación del responsable del propio usuario (o de la persona designada).

PROHIBIDA SU REPRODUCCION

9.3. Control de acceso lógico

Promotick deberá establecer una Política de contraseñas adecuada y alineada con las buenas prácticas en seguridad. La política de contraseñas definirá los requisitos de las contraseñas y los plazos de mantenimiento de una misma contraseña.

La Política de contraseñas deberá ser conocida por todos los empleados de Promotick.

9.4. Teletrabajo

Se deberá controlar el acceso remoto a la red de las sociedades de Promotick en la modalidad de trabajo a distancia, esto es, desde fuera de las instalaciones propias.

Los servicios de conexión al trabajo en remoto estarán destinados exclusivamente a personal de Promotick. Su uso por parte de cualquier otro tipo de colaborador requerirá autorización del responsable de seguridad.

El equipo utilizado para la conexión en la modalidad de trabajo en remoto podrá ser propiedad del empleado o proporcionado por Promotick. En cualquier caso, es obligatorio que el equipo cumpla con los siguientes requerimientos de seguridad:

a) Capacidad de realizar una conexión a través de una VPN.
b) Disponer de un sistema operativo actualizado con los últimos parches y actualizaciones de seguridad.
c) Software antivirus instalado.
d) Software de firewall/cortafuegos personal instalado.

El teletrabajo desde un equipo propio del trabajador requerirá de todas las medidas de seguridad oportunas, con el objetivo de que el trabajo en remoto no suponga una amenaza para la seguridad de la información de Promotick. Además, se podrán establecer medidas de seguridad adicionales a las existentes para asegurar de una manera más fiable la conexión segura en remoto.

El servicio de teletrabajo se monitorizará y controlará, registrándose tanto la conexión como la actividad de acuerdo con los protocolos de seguridad.

10. Gestión del ciclo de vida de la identidad

Promotick deberá definir e implementar un adecuado sistema de gestión del ciclo de vida de la identidad. La identidad es el conjunto de características que identifican de forma unívoca a toda persona con acceso físico o lógico a los sistemas de información de Promotick. El ciclo de vida de la identidad es el proceso que sigue la identidad de un usuario desde su creación hasta su eliminación.

El ciclo de vida de la identidad se compone de las siguientes actividades:

a) Creación y asignación de la identidad
b) Revisión periódica
c) Modificación o eliminación

PROHIBIDA SU REPRODUCCIÓN

La gestión de este ciclo requiere definir los requisitos de seguridad y responsabilidades de cada una de las etapas, con el objetivo de centralizar y facilitar los procesos de gestión asociados a las mismas.

La gestión del ciclo de vida de la identidad deberá estar alineado con el Departamento de RRHH con el objetivo de verificar las identidades en función de las altas y las bajas de empleados y su correspondencia en los sistemas de información.

10.1. Identidades Privilegiadas

La asignación y uso de derechos de acceso privilegiado deberá estar restringida y controlada. El acceso privilegiado es el acceso a sistemas como administrador o con un rol que ofrezca la posibilidad de modificarla configuración del sistema.

La asignación de derechos de acceso privilegiado deberá ser controlada a través de un proceso formal de autorización de acuerdo con las políticas de control de acceso. Deberán considerarse, al menos, los siguientes requisitos:

- Deberán identificarse los derechos de acceso privilegiados asociados a cada sistema o proceso (por ejemplo, sistema operativo, sistema de gestión de base de datos o aplicación), así como los usuarios a los que estos les deberán ser asignados.
- La asignación de derechos de acceso privilegiados deberá realizarse en base a las necesidades de uso, basándose en el mínimo privilegio y necesidad de saber.
- Deberá definirse un proceso de autorización que incluya un registro de los privilegios asignados. No deberán concederse derechos de acceso privilegiado hasta que el proceso de autorización se complete.
- Deberán definirse los requisitos para la caducidad de los derechos de acceso privilegiado.
- Las competencias de los usuarios con derechos de acceso privilegiado deberán revisarse regularmente con el objetivo de verificar que se encuentran alineadas con sus obligaciones.
- Deberán establecerse y mantenerse procedimientos y mecanismos específicos para evitar el uso no autorizado de cuentas de usuario genéricas para la administración, conformes con las capacidades de configuración de los sistemas.
- Se deberán establecer procedimientos y mecanismos que aseguren la confidencialidad de la información secreta de autenticación para los usuarios genéricos de administración (por ejemplo, modificación frecuente de contraseña, mecanismos de compartición de la contraseña seguros, etc.).

PROHIBIDA SU REPRODUCCION

11. Seguridad Física y del Entorno

Los espacios físicos donde se ubiquen los sistemas de información de Promotick deberán estar protegidos adecuadamente mediante controles de acceso perimetrales, sistemas de vigilancia y medidas preventivas de manera que puedan evitarse o mitigar el impacto de incidentes de Seguridad (accesos no autorizados a sistemas de información, robo o sabotaje) y accidentes ambientales (incendios, inundaciones, cortes de suministro eléctrico, etc.).

Además, deberá haber un control de acceso físico a la información que se encuentre en formato físico mediante un registro en papel sobre quién accede a la información. Por otra parte, la información confidencial se deberá almacenar con medidas específicas como armarios ignífugos.

12. Seguridad en trabajo en la nube o cloud

Promotick deberá mantener una política de trabajo en la nube o cloud computing que establezca las medidas de seguridad adecuadas para la confidencialidad, integridad y disponibilidad de la información. Dependiendo de tipo de modelo de servicio en la nube, se deberán aplicar diferentes medidas de seguridad:

- Infraestructura: en primer lugar, se deberá asegurar que el Proveedor monitoriza el entorno para detectar cambios no autorizados. Además, se deberán establecer fuertes niveles de autenticación y control de acceso para los administradores y las operaciones que estos realicen. Por último, las instalaciones y/o configuraciones de los elementos comunes deberán estar registrados y conectados con el objetivo de obtener la trazabilidad adecuada.
- Plataforma: de forma adicional a las medidas indicadas en el modelo de servicio de Infraestructura, el Proveedor del servicio deberá proporcionar mecanismos de seguridad correspondientes al ciclo de vida del software seguro, de acuerdo con el apartado *15. Seguridad en el ciclo de vida del desarrollo de sistemas*.
- Software: de forma adicional a las medidas indicadas en el modelo de servicio de Plataforma, Promotick y el Proveedor deberán seguir OWASP (Open Web Application Security) como guía para la seguridad de las aplicaciones.

13. Seguridad en la operativa

Todos los sistemas de información de Promotick que procesan o almacenan información de su propiedad deberán contar con las medidas de seguridad oportunas que optimicen su nivel de madurez adecuado (monitorización, control de cambios, revisiones, etc). Asimismo, se deberán gestionar, controlar y monitorizar las redes de manera adecuada, a fin de protegerse de las amenazas y mantener la seguridad de los sistemas y

PROHIBIDA SU REPRODUCCION

aplicaciones que utilizan la red, incluidos los controles de acceso a la red, protegiendo así toda la información que se transfiera a través de estos elementos y/o entornos.

14. Seguridad en las telecomunicaciones

La arquitectura de red de Promotick deberá contar con medidas de prevención, detección y respuesta para evitar brechas en los dominios internos y externos. Se entiende por “dominio interno” la red local compuesta por los elementos tecnológicos de Promotick accesibles exclusivamente desde la red interna. Por otra parte, se entiende por “dominio externo” la red accesible desde el exterior de la red de Promotick.

Es de suma importancia la administración de seguridad de las redes que atraviesan el perímetro de Promotick, implantando controles adicionales para los datos sensibles que circulen por las redes de comunicación públicas.

Por ello, Promotick definirá las pautas de seguridad a seguir con relación a la transferencia de información, así como las medidas de seguridad en la utilización de equipos portátiles, servicios de Internet y correo electrónico, y de controles específicos que permitan una conexión segura a los sistemas de información de Promotick desde fuera de sus instalaciones.

15. Seguridad en el ciclo de vida del desarrollo de sistemas

Toda la adquisición, desarrollo y mantenimiento de los sistemas deberá contar con unos requisitos mínimos de seguridad necesarios para el desarrollo de software, los sistemas y los datos acorde con las buenas prácticas del sector. Además, deberá realizarse una gestión de las pruebas, el seguimiento de los cambios, y el inventario del software.

Cada departamento de Promotick deberá tener en cuenta la seguridad de la información en sus procesos de sistemas y datos, procedimientos de selección, desarrollo e implementación de aplicaciones, productos y servicios.

15.1. Responsabilidad del Equipo de Desarrollo

El equipo de desarrollo es responsable de garantizar que todas las aplicaciones y sistemas cumplan con los principios y directrices establecidas por OWASP. Cada miembro del equipo deberá estar comprometido con la seguridad de la información y seguir las prácticas recomendadas por OWASP durante todo el proceso de desarrollo.

15.2. Evaluación de Riesgos

Antes de iniciar cualquier proyecto de desarrollo, se llevará a cabo una evaluación de riesgos utilizando la metodología OWASP. Se identificarán posibles vulnerabilidades y amenazas, y se tomarán medidas proactivas para mitigar los riesgos detectados.

PROHIBIDA SU REPRODUCCIÓN

15.3. Uso de Estándares OWASP

Se seguirán las guías y mejores prácticas proporcionadas por OWASP para el desarrollo seguro de aplicaciones web y sistemas. Estos estándares incluyen, pero no se limitan a, la Guía OWASP Top 10 y la Guía de Seguridad de Aplicaciones Web.

15.4. Protección de Datos

Todas las aplicaciones y sistemas desarrollados deberán implementar controles de seguridad para proteger los datos confidenciales. Se utilizará la encriptación adecuada para proteger los datos en reposo y en tránsito.

15.5. Gestión de Autenticación y Autorización

El acceso a las aplicaciones y sistemas se gestionará mediante una adecuada autenticación y autorización. Se implementarán controles de acceso basados en roles para asegurar que los usuarios solo tengan acceso a los recursos necesarios para su función.

15.6. Pruebas de Seguridad

Antes de poner en producción una aplicación o sistema, se realizarán pruebas de seguridad utilizando las herramientas y metodologías recomendadas por OWASP, incluyendo pruebas de penetración y análisis de vulnerabilidades.

15.7. Actualizaciones y Parches

Se establecerá un calendario para la aplicación de actualizaciones y parches de seguridad en todas las aplicaciones y sistemas desarrollados. El equipo de desarrollo se asegurará de mantener el software actualizado para protegerse contra vulnerabilidades conocidas.

15.8. Control de Versiones y Auditoría

Se implementará un sistema de control de versiones para el código fuente de todas las aplicaciones y sistemas desarrollados. Además, se mantendrán registros de auditoría para rastrear cambios en el código y posibles modificaciones no autorizadas.

PROHIBIDA SU REPRODUCCION

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

15.9. Cumplimiento Normativo

El equipo de desarrollo se asegurará de cumplir con todas las regulaciones y estándares de seguridad de la información aplicables, incluyendo aquellos relacionados con la protección de datos y privacidad.

15.10. Incumplimiento

El incumplimiento de esta política de desarrollo seguro puede resultar en acciones disciplinarias y consecuencias legales, dependiendo de la gravedad de la infracción.

16. Seguridad en los Proveedores

Se deberá poner especial atención en evaluar la criticidad de todos los servicios susceptibles de ser subcontratados de manera que puedan identificarse aquellos que sean relevantes desde el punto de vista de la seguridad de la información, ya sea por su naturaleza, la sensibilidad de los datos que deban tratarse o la dependencia sobre la continuidad de negocio.

Sobre los proveedores de estos servicios se deberán cuidar los procesos de selección, requerimientos contractuales como la terminación contractual, la monitorización de los niveles de servicio, la devolución de datos y las medidas de seguridad implantadas por dicho proveedor, que deberán ser, al menos, equivalentes a las que se establecen en la presente Política.

17. Gestión de Incidentes

Todos los empleados de Promotick tienen la obligación y responsabilidad de la identificación y notificación al responsable de seguridad de la sociedad de cualquier incidente o delito que pudiera comprometer la seguridad de sus activos de información. Asimismo, Promotick deberá implementar procedimientos para la correcta gestión de los incidentes detectados.

Se deberá definir un procedimiento de gestión de respuesta ante incidentes, en el que se defina un proceso de categorización de incidentes, análisis de impactos de negocio y escalado por parte de la función de seguridad de la información y ciberseguridad ante cualquier incidente relacionado con la seguridad de la información.

18. Continuidad de Negocio

Respondiendo a requerimientos de calidad y buenas prácticas, Promotick deberá disponer de un Plan de Continuidad de Negocio como parte de su estrategia para

PROHIBIDA SU REPRODUCCION

garantizar la continuidad en la prestación de sus servicios esenciales o críticos y el adecuado manejo de los impactos sobre el negocio ante posibles escenarios de crisis, proporcionando un marco de referencia para que la sociedad actúe en caso de ser necesario. Este Plan de Continuidad deberá ser actualizado y probado periódicamente. Además, se deberá definir y mantener actualizado un Plan de Recuperación ante Desastres alineado con la continuidad de negocio, este plan abarcará la continuidad del funcionamiento de las tecnologías de información y comunicación.

Promotick deberá encargarse de la formación y capacitación para todos sus empleados en materia de Continuidad del Negocio. La formación en materia de Continuidad del Negocio deberá ser revisada periódicamente con el objetivo de estar totalmente alineada con el Plan existente.

19. Cumplimiento regulatorio

Promotick deberá comprometerse a dotar los recursos necesarios para dar cumplimiento a toda la legislación y regulación aplicable a su actividad en materia de seguridad de la información y establecer la responsabilidad de dicho cumplimiento sobre todos sus miembros. En este sentido, se velará por el cumplimiento de toda legislación, normativa o regulación aplicable.

20. Auditorías de Seguridad y gestión de vulnerabilidades

Se deberá realizar una identificación periódica de vulnerabilidades técnicas de los sistemas de información y aplicaciones empleadas en la organización, de acuerdo a su exposición a dichas vulnerabilidades y adoptando las medidas adecuadas para mitigar el riesgo asociado.

Una vez identificadas las vulnerabilidades, la organización deberá aplicar las medidas correctoras necesarias tan pronto como sea posible. La identificación, gestión y corrección de las vulnerabilidades debe hacerse conforme a un enfoque basado en riesgos, teniendo en cuenta la criticidad y la exposición de los activos.

21. Gestión de Excepciones

Cualquier excepción a la presente Política de Seguridad de la Información deberá ser registrada e informada al responsable de la Seguridad de la Información de Promotick. Estas excepciones serán analizadas para evaluar el riesgo que podrían introducir a la sociedad y, en base a la categorización de estos riesgos, estos deberán ser asumidos por el peticionario de la excepción junto con los responsables del negocio.

PROHIBIDA SU REPRODUCCION

22. Sanciones disciplinarias

Cualquier violación de la presente Política de Seguridad de la Información puede resultar en la toma de las acciones disciplinarias correspondientes de acuerdo con el proceso interno de Promotick. Es responsabilidad de todos los empleados de Promotick notificar al responsable de Seguridad de la Información de la sociedad afectada cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas por la presente Política.

23. Revisión de la Política

La aprobación de esta Política implica que su implantación contará con el apoyo de la Dirección para lograr todos los objetivos establecidos en la misma, como también para cumplir con todos sus requisitos.

La presente Política de Seguridad de la Información, será revisada y aprobada anualmente por el Consejo de Administración. No obstante, si tuvieran lugar cambios relevantes en la sociedad o se identificaran cambios significativos en el entorno de amenazas y riesgos, ya sean estos de tipo operativo, legal, regulatorio o contractual, se procederá a su revisión siempre que se considere necesario, asegurando así que la Política permanece adaptada en todo momento a la realidad de Promotick.

PROHIBIDA SU REPRODUCCION

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

24. Anexos

24.1. Anexo: Niveles de clasificación

Nivel	Detalle Nivel	Ejemplos
Uso público	Se trata de la información que puede ser conocida por cualquier tipo de persona y su utilización fraudulenta no supone un riesgo para los intereses de Promotick.	Son ejemplos de este tipo de información los catálogos de productos y la información disponible en la página Web.
Difusión limitada	Es la información utilizada por las áreas de Promotick y cuya utilización fraudulenta supone un riesgo para los intereses de la empresa.	Son ejemplo de este tipo de información los correos electrónicos y los documentos de trabajo de las áreas de la empresa.
Información Confidencial	Es aquella información que solo puede ser conocida por un número reducido de personas y para la que un uso fraudulento puede suponer un impacto para los intereses de Promotick significativo.	Son ejemplos de este tipo de información los informes de auditoría y de estrategia de la empresa.
Información Reservada	Es la información que únicamente debe conocer el propietario de la misma y cuya divulgación puede suponer graves perjuicios para los intereses de la empresa.	Son ejemplos comunicaciones entre los altos directivos o accionistas con decisiones relevantes para la operativa de negocio.
Información Secreta	Es aquella cuya revelación no autorizada puede causar un perjuicio excepcionalmente grave a los intereses esenciales de la empresa.	Son ejemplos las claves criptográficas, información sobre fusiones o adquisiciones o cualquier otra información que pueda poner en riesgo el valor de la acción.

PROHIBIDA SU REPRODUCCION

activos. De esta forma se garantizará una evaluación correcta y precisa.

24.1. NIVELES Y CRITERIOS DE ACEPTACION DE RIESGOS

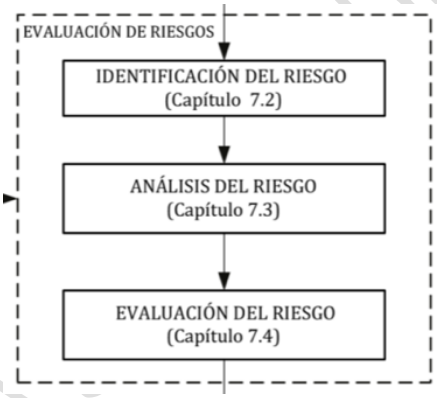
La organización en base a las buenas prácticas de gestión de riesgos ha establecido cinco niveles de riesgos los cuales son: **Muy Bajo, Bajo, Moderado, Alto y Muy Alto.** Así mismo de acuerdo con el análisis de su contexto interno y externo y las necesidades de las partes interesadas, se ha establecido que se aceptan aquellos riesgos de nivel

"Muy Bajo", "Bajo" y "Moderado", y no se aceptan los riesgos de nivel "**Alto" y "Muy Alto"** los cuales deben ser tratados.

En el caso de las Oportunidades se ha establecido que no se aceptan los niveles "Muy Baja", "Baja" y "Moderada", y se aceptan las Oportunidades de nivel "**Alta" y "Muy Alta**" las cuales deben ser tratadas.

24.2. EVALUACION DE RIESGOS Y OPORTUNIDADES

La **Evaluación** dentro de la **Gestión de Riesgos y Oportunidades** de seguridad de la información es el conjunto de actividades que permiten identificar, analizar, valorar y determinar un tratamiento.



PROHIBIDA SU REPRODUCCION

En cada fase del proceso es necesario realizar las actividades de seguimiento y revisión, así como las comunicaciones necesarias a las partes interesadas.

6.3.1. Identificación de riesgos y oportunidades del SGSI

En esta etapa se busca identificar dos aspectos:

- Los riesgos que tengan consecuencia en la efectividad del SGSI y la consecución de los objetivos de la organización.
- Las oportunidades que representen beneficios y apoyen con el cumplimiento de los objetivos del sistema de seguridad de la información en PROMOTICK PERÚ.

La identificación debe incluir todos los riesgos y oportunidades, sea que estén o no bajo el control de PROMOTICK PERÚ y debe ser permanente e interactivo basado en el resultado del análisis del Contexto, la planeación y los objetivos estratégicos de la organización.

Ir al punto 6.3.3.

Ver Anexo 1: Pasos para la identificación de Riesgos y Oportunidades del SGSI

6.3.2. Identificación de Riesgos de Seguridad de la Información

Los activos de información que hayan resultado con evaluación de **"crítico" y "muy crítico"** en la identificación realizada por el equipo son aquellos que requeriran ser parte de la identificación de riesgos. Se deben identificar los riesgos en concordancia con la evaluación CID realizada en la etapa previa.

Adicionalmente, para garantizar la no recurrencia del riesgo identificado, se deben de identificar también las amenazas y vulnerabilidades que provocan el riesgo identificado.

Ir al punto 6.3.4.

Ver Anexo 2: Pasos para la identificación de Riesgos de Seguridad de la Información

6.3.3. Análisis de Riesgos y Oportunidades del SGSI

El análisis de los riesgos y oportunidades del SGSI busca establecer la *probabilidad* (posibilidad de ocurrencia) y la consecuencia/impacto (magnitud de los efectos que puede ocasionar) si se materializan, con el fin de obtener información para determinar el nivel de riesgos y el nivel de oportunidad respectivamente.

Para tal fin, se han desarrollado escalas con los niveles respectivos de Probabilidad e Impacto.

PROHIBIDA SU REPRODUCCION

Ir al punto 6.3.5.

Ver Anexo 3: Criterios y pasos para el análisis de Riesgos y Oportunidades.

6.3.4. Análisis de Riesgos de Seguridad de la Información

El análisis de los riesgos de seguridad de la información establece la probabilidad de ocurrencia del riesgo para la organización y los niveles en los que afecta la Confidencialidad, Integridad y Disponibilidad del activo, en caso el riesgo se materialice. Mediante este análisis se obtiene el nivel de riesgo.

Las escalas CID de evaluación están definidas en el anexo 3: Criterios y pasos para el análisis de Riesgos y Oportunidades.

Ir al punto 6.3.5.

6.3.5. Valoración de Riesgos y Oportunidades

La valoración es el proceso de comparar el nivel del riesgo contra los criterios de aceptación de riesgo. En este caso, se ha determinado que la organización acepta riesgos y oportunidades con un nivel **Muy Bajo, Bajo y Medio**.

6.3.6. Plan de Tratamiento de Riesgos y Oportunidades

Para cada riesgo y oportunidad clasificado en la etapa anterior se deberá completar en la matriz correspondiente las acciones determinadas para tratar dichos riesgos y oportunidades.

En esta etapa se definen las acciones a seguir ante los riesgos y oportunidades. Deben tener asignado un responsable de realizarlas y un responsable de verificar su cumplimiento en un plazo comprometido (dueño del riesgo). El plan se presenta a la gerencia quien lo aprueba o realiza los cambios necesarios. La aprobación se puede dar mediante la impresión y firma del plan de tratamiento, por correo electrónico o firmando el acta de reunión en donde se revisó.

Ver Anexo 4: Tratamiento de Riesgos y Oportunidades

PROHIBIDA SU REPRODUCCION

24.3. RIESGO RESIDUAL DE LOS RIESGOS DE S.I. Y EFECTIVIDAD DEL PLAN DE ACCION DE LOS RIESGOS Y OPORTUNIDADES DEL SGSI

Una vez implementada la acción (el plan de tratamiento) se debe revisar si se logró el efecto deseado. Es decir, se debe evaluar el riesgo residual (riesgos de seguridad de la información) y en el caso de los riesgos y oportunidades del SGSI, ver si fueron eficaces.

La forma de determinar el riesgo residual es volver a realizar el proceso de valoración de riesgos considerando los controles implementados y determinando el Nivel de Efectividad del Control (Matriz de Riesgos, sección Riesgo Residual), con la información del nuevo control, se procede a analizar la probabilidad y el impacto, determinando el Nivel del Riesgo Residual.

La efectividad del riesgo residual es llegar al nivel “Muy Bajo” o “Bajo”, los cuales son aceptados.

El Nivel de Riesgo Residual “Moderado” es tolerable, en este caso, la organización decide si continúa implementando controles o lo acepta.

Los Niveles de Riesgo Residual “Muy Alto” y “Alto” no son aceptables, en este caso, se tendrían que seguir implementando controles hasta llegar al nivel aceptable.

En el caso de los Riesgos y Oportunidades del SGSI, se evalúa la eficacia revisando los beneficios obtenidos por su implementación y se registra en la matriz, columna “Eficacia”

Los riesgos residuales y la eficacia se presentan a la gerencia quien los aprueba previa revisión. La aprobación se puede dar mediante la impresión y firma del plan de tratamiento y Riesgo Residual, por correo electrónico o firmado el acta de reunión en donde se revisó.

24.4. SEGUIMIENTO Y REVISIÓN

Se realizará un seguimiento constante a cada una de las fases de la Gestión de Riesgos y Oportunidades con motivos del cumplimiento del mismo. El seguimiento estará a

PROHIBIDA SU REPRODUCCION

cargo de cada propietario del riesgo y/u oportunidades involucrado y del Coordinador de Seguridad de la Información.

Se debe actualizar la Evaluación de riesgos y oportunidades por lo menos una vez al año o cada vez que se presente:

- Cambios relevantes en la organización
- Cambios en los objetivos y procesos
- Solicitud de la Dirección
- Otros

Los resultados del seguimiento y revisión serán registrados y servirán de información de entrada para la evaluación de la Gestión de Riesgos y Oportunidades.

7. COMUNICACIÓN Y CONSULTA

La comunicación y consulta estará presente en todas las fases de la Gestión de Riesgos y Oportunidades con las partes interesadas internas y externas. Como los juicios de las partes interesadas tendrán un impacto significativo en las decisiones tomadas deben ser registrados y tomados en cuenta en toda decisión dentro del proceso.

8. ANEXOS

ANEXO 1: Pasos para la identificación de Riesgos y Oportunidades del SGSI

Para la identificación de Riesgos y Oportunidades la organización debe de haber establecido el contexto interno y externo en el documento **SGSI-DG-001 Contexto Interno, Externo y Partes Interesadas**. Este debe contemplar también un análisis FODA que apoye en la identificación de Riesgos y Oportunidades que afecten al Sistema de Gestión de la Seguridad de la Información.

PROCESO DE EVALUACIÓN

El proceso se divide en dos:

- Evaluación de oportunidades
- Evaluación de riesgos.

PROHIBIDA SU REPRODUCCION

El Proceso de Evaluación de Riesgos consiste en la identificación, partes afectadas y valoración sistemática de los riesgos asociados a una actividad, así como al SGSI mismo.

Para que el proceso sea realizado de una manera ágil, la cuantificación del impacto se realizan de forma cualitativa, es decir, se asignan valores subjetivos que están en concordancia con el conocimiento y experiencia que tienen los integrantes del equipo de evaluación de riesgos y del responsable del proceso analizado.

El proceso de Evaluación de Oportunidades consiste en la identificación, parte afectada y valoración de mejoras que pueden beneficiar a la organización.

Para que estos procesos sean efectivos, se requiere la participación de los encargados de las diversas áreas.

Una vez identificados y gestionados los Riesgos y Oportunidades, se debe realizar nuevamente este proceso, es recomendable repetir el proceso por lo menos una vez al año, cuando la dirección lo determine o cada vez que un evento produzca cambios relevantes en un área o proceso determinado.

IDENTIFICACIÓN DE RIESGOS Y OPORTUNIDADES

Es el proceso mediante el cual se identifican propiamente los Riesgos y Oportunidades dentro del proceso a analizar. En el caso de riesgos, esta fase tiene como objetivo identificar los riesgos que afectan los diferentes procesos y también que pueden afectar el desempeño del Sistema de Gestión de Seguridad de la Información. La evaluación es realizada por el Coordinador de Seguridad de la Información en coordinación con los encargados de los procesos de PROMOTICK PERÚ. Se debe determinar a qué partes interesadas afectaría el riesgo de materializarse.

En el caso de las oportunidades se describe la oportunidad, que fortaleza apoya a la oportunidad establecida y a que parte interesada beneficiaría de explotar la Oportunidad.

PROHIBIDA SU REPRODUCCION

MÉTODO DE IDENTIFICACIÓN DE RIESGOS Y OPORTUNIDADES

Participantes

Durante las actividades de identificación y análisis deberán participar:

- El responsable de los diferentes procesos de la organización.
- Otros colaboradores claves de las áreas a las que se realizará la identificación y valoración.
- Coordinador de Seguridad de la Información y equipo de trabajo definido previamente. Incluye la posibilidad de trabajar de la mano de consultores especializados en Evaluaciones de Riesgos de Seguridad de la Información.

Actividades

En primer lugar, se establecen reuniones de trabajo al estilo talleres donde los participantes se enfocarán en la identificación y valoración de riesgos y oportunidades.

Las reuniones deben ser previamente coordinadas y durarán un estimado de dos horas, la propuesta de tiempo varía de acuerdo con el alcance del proceso o. Es importante tener el apoyo de la Alta Dirección para que los talleres tengan por lo menos un 90% de asistencia en general.

En el caso de los riesgos de la organización se identifica:

- Descripción del riesgo
- Contexto del que proviene
- Partes Interesadas a las que afecta
- Análisis del Riesgo:
  - Probabilidad de ocurrencia del riesgo
  - Impacto del Riesgo
  - Nivel del riesgo
- Opción de Tratamiento
- Tratamiento
  - Actividades
  - Responsables
  - Fecha de inicio y fin
  - Estado de implementación
  - Determinación de efectividad
  - Evidencias de la efectividad.

PROHIBIDA SU REPRODUCCION

En el caso de las oportunidades de de la organización, se identifica:

- Descripción de la oportunidad
- Fortaleza que soporta a la oportunidad
- Contexto del que proviene
- Parte interesada a la que beneficiaría
- Analisis de la oportunidad:
  - Probabilidad de ocurrencia
  - Impacto de la oportunidad
  - Nivel de la oportunidad
- Opción de tratamiento
- Tratamiento:
  - Actividades
  - Responsables
  - Fecha de inicio y fin
  - Estado de implementación
  - Determinación de efectividad
  - Evidencias de efectividad

Documentación

Se documentará la información levantada mediante el formato **SGSI-FOR-005 Matriz de Riesgos y Oportunidades del SGSI.** En caso se manejen servicios de consultoría para la Gestión de Riesgos la realización de Actas de Reunión es obligatoria para todas las reuniones del proceso. Esto servirá tambien de apoyo para la aprobación de las actividades a realizar por parte de los responsables.

PROHIBIDA SU REPRODUCCION

ANEXO 2: Pasos para la identificación de Riesgos de Seguridad de la Información

Para el caso de Riesgos, se deben de considerar los Activos de Información identificados en el inventario de activos de información de la organización que hayan tenido como resultado de la valoración en la escala CID por los propietarios como “críticos” y “muy críticos”.

PROCESO DE EVALUACIÓN

El Proceso de Evaluación de Riesgos consiste en la identificación, análisis y valoración sistemática de los riesgos asociados a una actividad y a un grupo de activos o activo de información de la organización.

Para que el proceso sea realizado de una manera ágil, la cuantificación del impacto y las vulnerabilidades se realizan de forma cualitativa, es decir, se asignan valores subjetivos a la afectación de la Confidencialidad, Integridad y Disponibilidad que están en concordancia con el conocimiento y experiencia que tienen los integrantes del equipo de evaluación de riesgos, del responsable del proceso analizado y del propietario del riesgo.

Una vez identificados y gestionados los Riesgos, se debe realizar nuevamente este proceso, es recomendable repetir el proceso por lo menos dos veces al año, cuando la dirección lo determine o cada vez que un evento produzca cambios relevantes en un área o proceso determinado.

IDENTIFICACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Es el proceso mediante el cual se identifican propiamente los riesgos de seguridad de la información. Esta fase tiene como objetivo identificar los riesgos de seguridad de la información a los que están expuestos los activos críticos y muy críticos, la Fuente del riesgo, sus causas, sus orígenes, consecuencias, determinar el dueño del riesgo, los controles a implementar, sus niveles de efectividad y áreas/procesos vinculadas(os) de la organización. La estimación es realizada por el Coordinador de Seguridad de la Información en coordinación con los responsables de los Activos de Información (Propietarios y Custodios de la información) de PROMOTICK PERÚ.

PROHIBIDA SU REPRODUCCION

MÉTODO DE IDENTIFICACIÓN DE RIESGOS Y OPORTUNIDADES

Participantes

Durante las actividades de identificación y análisis deberán participar:

- El responsable de los activos de información de acuerdo a los procesos a evaluar.
- Otros colaboradores claves de las áreas a las que se realizará la identificación y análisis.
- Coordinador de Seguridad de la Información y equipo de trabajo definido previamente. Incluye la posibilidad de trabajar de la mano de consultores especializados en Evaluaciones de Riesgos de Seguridad de la Información.

Actividades

En primer lugar, se establecen reuniones de trabajo al estilo talleres donde los participantes se enfocarán en la identificación y análisis de riesgos y oportunidades.

Las reuniones deben ser previamente coordinadas y durarán un estimado de dos horas, la propuesta de tiempo varía de acuerdo con el alcance del proceso o áreas a evaluar. Es importante tener el apoyo de la Alta Dirección para que los talleres tengan por lo menos un 90% de asistencia en general.

En el caso de los riesgos de los procesos internos se identifica:

- Fecha de Identificación
- El proceso afectado
- Activo al que afecta el riesgo
- Causa Raíz / Amenaza
- Vulnerabilidad
- Código de Riesgo
- La descripción del riesgo
- Las consecuencias
- Propietario del riesgo
- Control actual implantado
- Cumplimiento del control
- Probabilidad de ocurrencia del riesgo
- Evaluación del riesgo
  - Confidencialidad
  - Integridad
  - Disponibilidad
- Impacto del Riesgo

PROHIBIDA SU REPRODUCCION

- Nivel del riesgo
- Estrategia de respuesta
- Nivel de Priorización

Documentación

Se documentará la información levantada mediante el formato **SGSI-FOR-007 Matriz de riesgos de seguridad de la información**. En caso se manejen servicios de consultoría para la Gestión de Riesgos la realización de Actas de Reunión es obligatoria para todas las reuniones del proceso.

PROHIBIDA SU REPRODUCCION

ANEXO 3: Criterios y pasos para el análisis de Riesgos y Oportunidades

Para esta actividad, se deben de establecer criterios y niveles para evaluar la probabilidad e impacto de riesgos y oportunidades. Así mismo se deben de establecer los niveles de Exposición de los riesgos y oportunidades.

En el caso de los Riesgos de Seguridad de la Información, se ha establecido identificar y analizar las amenazas y las vulnerabilidades. Así mismo se debe revisar como parte del análisis los controles implementados y su nivel de efectividad.

Una **Amenaza** es un evento accidental o intencionado que pueda ocasionar algún daño a los activos de información o a la información relacionada a ellos.

Una **Vulnerabilidad** es cualquier debilidad en los mecanismos de protección (controles) de los activos que pueda permitir a las amenazas causarle daños y producir pérdidas en la empresa.

En el caso de las Oportunidades, se analiza el beneficio que se obtendría. El Nivel de Exposición se calcula con el **producto de la probabilidad de ocurrencia por el impacto.**

Nivel de Riesgo / Oportunidad del SGSI

Para identificar el Nivel de Riesgo y Oportunidad, se considera el uso de las siguientes tablas:

MATRIZ DE RIESGOS					
MAPA DE CALOR DE RIESGOS					
PROBABILIDAD					
5 Casi Cierto	Bajo	Medio	Alto	Muy Alto	Muy Alto
4 Probable	Bajo	Medio	Medio	Alto	Muy Alto
3 Posible	Muy Bajo	Bajo	Medio	Medio	Alto
2 Improbable	Muy Bajo	Bajo	Bajo	Medio	Medio
1 Raro	Muy Bajo	Muy Bajo	Muy Bajo	Bajo	Bajo
	1 Muy Bajo	2 Bajo	3 Moderado	4 Alto	5 Muy Alto
	IMPACTO				

PROHIBIDA SU REPRODUCCION

MATRIZ DE OPORTUNIDADES					
MAPA DE CALOR DE OPORTUNIDADES					
PROBABILIDAD					
5 Realizable	**Baja**	**Moderada**	**Alta**	**Muy Alta**	**Muy Alta**
4 Probable	**Baja**	**Moderada**	**Moderada**	**Alta**	**Muy Alta**
3 Posible	**Baja**	**Baja**	**Moderada**	**Moderada**	**Alta**
2 Improbable	**Baja**	**Baja**	**Baja**	**Moderada**	**Moderada**
1 No Realizable	**Baja**	**Baja**	**Baja**	**Baja**	**Baja**
	1 Muy Bajo	2 Bajo	3 Moderado	4 Alto	5 Muy Alto
	IMPACTO				

A continuación, se describe a detalle los dos vectores que se utilizan para clasificar a los riesgos y Oportunidades:

Probabilidad de Ocurrencia

Para determinar la probabilidad de ocurrencia, se considera el detalle de la siguiente tabla:

PROHIBIDA SU REPRODUCCIÓN

Clasificación	Oportunidad
No Realizable	La probabilidad que se pueda realizar es nula.
improbable	**Podría realizarse** Existen condiciones que hacen que su probabilidad de realización sea a largo plazo.
Posible	**Puede ocurrir su realización.** Existen condiciones que hacen poco probable la realización en el corto plazo (1 año) pero que no son suficientes para evitarlo en el largo plazo.
Probable	**Probablemente se realice.** Se puede dar en el corto plazo y no existen condiciones que impidan la ocurrencia.
Realizable	Se puede realizar en la mayoría de las circunstancias. La ocurrencia es inminente.

Clasificación	Riesgo
Raro	Puede ocurrir en circunstancias excepcionales; una vez cada dos años. / No existen condiciones que impliquen riesgo.
Improbable	Podría ocurrir una vez cada dos años. / Existen condiciones que hacen lejana la posibilidad de ocurrencia.
Posible	Puede ocurrir una vez al año. / Existen condiciones que hacen poco probable en el corto plazo pero que no son suficientes para evitarlo en el largo plazo.
Probable	Probablemente ocurrirá una vez al mes. / No existen condiciones que impidan la ocurrencia.
Casi Cierto	Ocurrirá en la mayoría de las circunstancias; varias veces al mes. / La ocurrencia es inminente.

PROHIBIDO REPRODUCCION

Impacto

Para determinar el nivel del impacto, se considera el detalle de la siguiente tabla:

Clasificación	Oportunidad
Muy Bajo	Impacto no significativo, no beneficiaria el logro de objetivos de la compañía o terceros. No impacta en los proceso.
Bajo	Impacto no significativo. Beneficiaria con un margen mínimo el logro de objetivos de la compañía o terceros. El impacto es mínimo en los procesos.
Moderado	Impacto que podría ocasionar un beneficio para el logro de objetivos de la compañía o terceros hasta a un 50% El impacto es moderado en los procesos.
Alto	Impacto que podría ocasionar en beneficio para el logro de objetivos de la compañía o terceros a un 100%. El impacto es alto en los procesos.
Muy Alto	Impacto que podría ocasionar un beneficio para el logro de objetivos de la compañía o terceros a un 100% y que además genera nuevas oportunidades en el ámbito de tecnología y de negocio. El impacto es critico en los procesos.

PROHIBIDA

Clasificación	Riesgo
Muy Bajo	Impacto insignificativo, no afectaría actividades ni procesos de la organización o terceros.
Bajo	Impacto insignificativo, afectaría una actividad o proceso no críticos de la organización o terceros.
Moderado	Impacto que podría ocasionar un perjuicio en una actividad o proceso crítico o más de una actividad o proceso no crítico de la organización o terceros.
Alto	Impacto que podría ocasionar un perjuicio significativo para la organización o terceros y que podría impedir la ejecución de las actividades de la organización.
Muy Alto	Impacto que podría ocasionar un perjuicio significativo para la organización o terceros y que podría impedir la ejecución de las actividades de la organización, incumplimientos legales, regulatorios, normativos, hay multas y/o sanciones

Por último, a **cualquier riesgo u oportunidad representado en la Matriz SGSI-FOR-005 Matriz de Riesgos y Oportunidades del SGSI que resulte Alto o Muy Alto se le realizará el Plan de Tratamiento.** El resto de los riesgos inmediatamente se aceptarán por no ser significativos. En el caso de las oportunidades, estas no se tomarán en cuenta.

Nivel de Riesgo de Seguridad de la Información

Para identificar el Nivel de Riesgo de Seguridad de la Información, se considera el uso de las siguientes tablas:

PROHIBIDA SU REPRODUCCIÓN

Figura : Mapa de calor de los Riesgos

PROBABILIDAD					
	10. Muy Alto	40. Medio	60. Alto	80. Muy Alto	100. Muy Alto
	8. Alto	32. Medio	48. Alto	64. Alto	80. Muy Alto
	6. Media	24. Bajo	36. Medio	48. Alto	60. Alto
	4. Baja	16. Bajo	24. Bajo	32. Medio	40. Medio
		4. Bajo	6. Medio	8. Alto	10. Muy Alto
		CONSECUENCIA			

A continuación se detallan las escalas de evaluación CID utilizadas para obtener los niveles de riesgo:

Nivel de Probabilidad:

Nivel	Clasificación	Riesgo
4	Baja	Puede ocurrir en circunstancias excepcionales; una vez cada dos años. / No existen condiciones que impliquen riesgo.
6	Media	Puede ocurrir una vez al año. / Existen condiciones que hacen poco probable en el corto plazo pero que no son suficientes para evitarlo en el largo plazo.
8	Alta	Probablemente ocurrirá una vez al mes. / No existen condiciones que impidan la ocurrencia.
10	Muy Alta	Ocurrirá en la mayoría de las circunstancias; varias veces al mes. / La ocurrencia es inminente.

PROHIBIDO REPRODUCCIÓN

Escalas de impacto:

Nivel	Clasificación	Confidencialidad
0	No hay impacto	No se presenta impacto alguno a la confidencialidad de los activos. No afecta en ninguna medida las actividades o procesos de la organización o terceros
4	Bajo	Impacto insignificativo a la confidencialidad de los activos, afectaría una actividad o proceso no críticos de la organización o terceros.
6	Medio	Impacto que podría afectar a la confidencialidad de los activos, ocasionar un perjuicio en una actividad o proceso crítico o más de una actividad o proceso no crítico de la organización o terceros.
8	Alto	Impacto que podría afectar a la confidencialidad de los activos, ocasionar un perjuicio significativo para la organización o terceros y que podría impedir la ejecución de las actividades de la organización.
10	Muy Alto	Impacto que podría afectar a la confidencialidad de los activos, ocasionar un perjuicio significativo o catastrófico para la organización, terceros o podría impedir la ejecución de las actividades de la organización, incumplimientos legales, regulatorios, normativos, hay multas y/o sanciones

PROHIBIDA SU REPRODUCCIÓN