POLITICA DE SEGURIDAD DE LA INFORMACION

CONSEJEROS Y CORREDORES DE SEGUROS S.A.

Consejeros
CORREDORES DE SEGUROS

2025

OBJETIVO

OBJETIVO

Establecer un marco general de seguridad de la información que permita lograr los niveles de seguridad en conformidad con la norma ISO/IEC 27001:2022para el SGSI de la empresa.

ALCANCE

ALCANCE

Aplica a todos las áreas, colaboradores y terceros relevantes que formen parte o brinden servicios a la empresa.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

CONSEJEROS en cumplimiento con su misión, visión y valores y comprometido con la mejora continua de sus procesos y generando valor económico, social y ambiental para el desarrollo del país, establece la implementación del SGSI (Sistema de Gestión de Seguridad de la Información) y se compromete a:

- Proteger los activos de información frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información.
- Proporcionar los recursos necesarios para asegurar la implementación de las medidas de control necesarias para evitar que los riesgos de la seguridad de la información se materialicen.
- Mejorar el nivel de conciencia de seguridad de la información en los gerentes, jefes, terceros, colaboradores y usuarios de los servicios de la organización.
- Mejorar continuamente la eficacia del SGSI a fin de minimizar de manera constante los riesgos de la seguridad de la información.
- Cumplir con los requisitos legales y regulatorios que afectan a la organización respecto a la seguridad de la información.
- Establecimiento y cumplimiento de los requisitos contractuales con las partes interesadas.
- Establecimiento de las consecuencias de las violaciones a la política de seguridad de la información, las cuales serán reflejadas en los contratos firmados con las partes interesadas, proveedores y empleados.
- Proporcionar el marco de referencia para la mejora continua del Sistema de Gestión de Seguridad de la Información.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

- Nuestro Sistema de Seguridad de la Información profundiza los diversos requisitos en documentos específicos, a continuación, nombramos algunos:
  - SGSI-MA-GN-01 Manual de roles y responsabilidades de seguridad de la información → Especifica las responsabilidades en materia de seguridad de la información de la alta dirección, comité del SGSI, OSI, propietarios de riesgos y oportunidades, gerentes, colaboradores y proveedores.
  - SGSI-MET-GN-01 Gestión de riesgos y oportunidades → Especifica la metodología para identificar, medir, establecer planes de acción para mitigar dichos riesgos y potenciar las oportunidades.
  - SGSI-PR-GN-08 Procedimiento de gestión de accesos lógicos → Especifica el proceso para el alta, modificación y baja de accesos.
  - SGSI-PR-GN-09 Gestión de incidentes de seguridad de la información → Especifica el proceso para gestionar los incidentes de seguridad de la información que ocurriesen en la organización.
  - SGSI-FO-GN-07 Formato Plan de comunicaciones-concientización para el SGSI → Especifica la planificación de las comunicaciones, capacitaciones, boletines y recordatorios que contribuyan a la concientización de la organización en materia de seguridad de la información.
  - SCN-MA-CP-01 Plan de Continuidad del Negocio → Especifica los procesos, actividades y servicios críticos de la empresa, la identificación de los diferentes escenarios disruptivos, la probabilidad y el impacto en caso ocurran, describir los planes de respuesta ante dichas situaciones, especificando el proceso a seguir para retomar las actividades y que el negocio no se vea perjudicado en ningún momento.
  - SGSI-PR-GN-06 Procedimiento de monitoreo, medición, análisis y evaluación del SGSI → Especifica el monitoreo a través de diferentes indicadores de medición que nos dan información sobre el desempeño del sistema.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

- SGSI-PR-GN-05 Procedimiento de auditoría interna al SGSI → Especifica el proceso de revisión de manera interna a nuestros procesos, documentación, registros e indicadores que permite identificar hallazgos y oportunidades de mejora con la finalidad de mejorar continuamente.
- El detalle del funcionamiento de nuestro sistema se encuentra en nuestros manuales: SGSI-MA-GN-03 Manual del SGSI y SGSI-MA-GN-02 Manual de controles de seguridad de la información.

Esta Política proporciona el marco de referencia para la mejora continua del Sistema de Gestión de Seguridad de la Información; así como, para establecer y revisar los objetivos del mismo; siendo comunicada a toda la Organización a través de su publicación y difusión interna; revisada anualmente para su adecuación o, extraordinariamente cuando concurran situaciones especiales o cambios sustanciales, estando disponible para las partes interesadas a través de su publicación externa.

Medidas de Control de Consejeros:

Como manifestación del poder de dirección contenido en el artículo 9° del DS 03-97-TR – TUO de la Ley de Productividad y Competitividad Laboral, CONSEJEROS podrá establecer medidas de control sobre todas las herramientas informáticas proporcionadas como parte del SGSI.
Las medidas de control seguirán las siguientes etapas:
·ETAPA PREVIA: Consiste en la etapa mediante la cual CONSEJEROS realiza un control superficial a las herramientas tecnológicas. Mediante el apoyo de una solución tecnológica de auditoría se filtra la capa base de la información transmitida y/o recibida en las distintas herramientas tecnológicas, como por ejemplo asuntos, destinatarios y fechas de correos, historial de visitas, etc.

La etapa previa busca afianzar, mediante un sistema de auditoría, un control base sobre la información transmitida en las herramientas proporcionadas por CONSEJEROS. En esta etapa no se tiene acceso al contenido de archivos, conversaciones, correos, etc.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La etapa previa busca afianzar, mediante un sistema de auditoría, un control base sobre la información transmitida en las herramientas proporcionadas por CONSEJEROS. En esta etapa no se tiene acceso al contenido de archivos, conversaciones, correos, etc.

·ETAPA DE INTERVENCIÓN MODERADA: Dependiendo del resultado de la etapa previa, siempre que se adviertan indicios sustentables que atenten contra la política de seguridad de la información, podrá recurrirse a una intervención moderada que implica la posibilidad de acceder al contenido de cualquier comunicación que implique una transmisión de información observada.

·ETAPA DE INTERVENCIÓN TOTAL: En caso se advierta un nivel de riesgo alto respecto a la política de seguridad de la información, CONSEJEROS se encontrará facultado para intervenir y fiscalizar de forma total cualquier herramienta proporcionada por la organización.

Del resultado de las medidas de control, podrán advertirse una serie de incumplimientos detallados en el proceso disciplinario de Seguridad de la Información, los mismos que únicamente tienen carácter enunciativo más no limitativo. Asimismo, se deberá considerar que, dependiendo de los hallazgos y la información recabada, podrán advertirse los incumplimientos desde la primera etapa de control. La aplicación sucesiva de las etapas requerirá de una justificación razonable y de un riesgo inminente para la seguridad de la información de CONSEJEROS.

INCUMPLIMIENTO DE LA POLÍTICA

CONSEJEROS hará responsable al trabajador de las consecuencias derivadas por el incumplimiento de las políticas y normas establecidas en este documento. Cualquier acción disciplinaria derivada del incumplimiento de la misma será considerada de acuerdo al procedimiento del SGSI-DG-AD-01 Proceso disciplinario para la seguridad de la información. El trabajador que no cumpla con el uso correcto de los activos será directamente responsable de las sanciones legales derivadas de sus propios actos y de los costos y gastos en que pudiera incurrir la empresa en defensa por el uso no autorizado o indebido de los recursos.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA USUARIOS

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA USUARIOS

Política de Dispositivos Móviles

- Las características en las capacidades de los equipos deberán ser definidos en función de la importancia de la información procesada o almacenada en cada tipo de usuario que utiliza un dispositivo móvil de la organización.
- Todos los usuarios de dispositivos móviles que contengan información confidencial o de uso interno deben usar la última o la más segura versión de los productos de software. Los parches o actualizaciones serán obtenidos de manera formal, provenientes del fabricante.
- Se debe mantener actualizado el software antivirus de los dispositivos móviles.
- Los colaboradores deben hacer uso de los dispositivos móviles (si se les son asignados) de la empresa, no está permitido que los colaboradores hagan uso de dispositivos que no fueron asignados por la empresa.
- Los nuevos dispositivos son configurados con las medidas necesarias antes de ser entregados al usuario final.
- La empresa puede recuperar mensajes borrados y guardar copias de seguridad de los celulares entregados.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA USUARIOS

Política Para el Uso Aceptable de los Activos

- El uso de la información y de los activos de información debe ser para propósitos de las actividades de la empresa de acuerdo con las políticas, procedimientos o cualquier lineamiento que definan.
- No se debe divulgar información que haya sido clasificada como confidencial o restringida, salvo autorización del propietario de información quien debe ser responsable de la divulgación.
- Cualquier acceso, modificación o eliminación de información o de un activo de información debe ser expresamente autorizada por el propietario de información o propietario del activo de información.
- Se deben cumplir con lo establecido en los requisitos legales, contractuales y normativos relativos al uso de activos de información.
- El personal que ponga en riesgo los activos de información, se le aplicará medidas disciplinarias de acuerdo con el proceso disciplinario vigente.
- Todos los activos a los que tenga acceso un personal se encuentran bajo su responsabilidad y deben de proteger su integridad y confidencialidad.
- Todo activo que contiene información no debe ser desatendido, debe quedar resguardado bajo llave o se deben utilizar bloqueos especiales para asegurarlo.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA USUARIOS

- Todo incidente de seguridad de la información que involucre a información confidencial o a los activos que soportan dicha información deben ser reportados por los canales establecidos.

Política Para la Gestión de Medios Removibles

Se ha establecido la siguiente política específica para el uso de medios removibles que contienen información clasificada como “confidencial” o “restringida”:

- Los usuarios que usen medios removibles como memorias USB, discos externos, DVDs y CDs deben evitar utilizarlos en equipos internos o externos que no cuenten con las medidas de seguridad mínimas requeridas como un antivirus y de ser necesario solicitar al departamento de Soluciones de Tecnología la implementación de controles de cifrado. Además, son responsables del aseguramiento físico de estos, en tal sentido, cuando no se estén usando deben quedar resguardados en un cajón con llave u otro espacio seguro.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA USUARIOS

- Los medios removibles no deben quedarse conectados en equipos desatendidos por largos períodos de tiempo.
- Los medios removibles deben ser devueltos por cese o cambio de posición de personal, y se debe realizar el borrado seguro de la información contenida en el medio.

Política de Control de Accesos

- El control de acceso a los sistemas de información debe realizarse por medio de códigos de identificación y contraseñas únicos para cada usuario. Las cuentas de usuario deben ser únicas para cada empleado y éste será responsable por toda actividad que sea realizada con dicho usuario.
- Se establece que el uso de contraseñas robustas debe estar configurado en los sistemas de información.
- Está prohibido intentar ingresar a la infraestructura tecnológica con la cuenta de usuario de otro empleado.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA USUARIOS

- El nivel de acceso a un sistema de información se otorgará de acuerdo con:
  - La clasificación de la Información.
  - Funciones del usuario.
  - Perfiles de acceso estandarizados.
  - Pedido, autorización y administración de acceso.
  - Revisión periódica.
  - Retiro y modificación de derechos de acceso.
- Los sistemas de información, según su criticidad y uso, deberían desconectar automáticamente las sesiones de conexión tras un periodo definido de inactividad que sea configurable por cada sistema.
- Los usuarios no pueden descargar/ instalar programas sin autorización; las instalaciones deben hacerlas únicamente el personal responsable de ello.
- El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información debe ser asignado de acuerdo con la identificación previa de requerimientos de la organización y de seguridad de la información.
- Todos y cada uno de los equipos de cómputo deben ser asignados a un responsable, por lo que es de su competencia hacer buen uso de estos.
- Los accesos con altos privilegios (usuarios administradores) deben ser controlados igualmente mediante un procedimiento formal.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA USUARIOS

- Periódicamente se debe revisar que los accesos de las cuentas de usuario de personal cesado hayan sido eliminados y/o deshabilitados.
- Periódicamente se debe revisar que los accesos concedidos a los usuarios sean los que les corresponde de acuerdo con las funciones que desempeñan.
- El acceso a repositorios con código fuente debe ser controlado.

Política de Uso de Controles Criptográficos

- Se deberán utilizar controles criptográficos en los siguientes casos:
  - Para el uso de firmas digitales y certificados digitales.
  - Para el resguardo de información, cuando así resulte de la evaluación de riesgos realizada por el Propietario de Activo de Información o Propietario del Riesgo; cuando la información saldrá de la empresa en un medio extraíble.
  - La encriptación de los archivos y datos se realiza mediante el algoritmo AES y los archivos se guardan con extensión .bin

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA USUARIOS

Política de Equipos de Usuario Desatendidos

- Al dejar un equipo desatendido temporalmente, el usuario debe bloquear el acceso a su computador, laptop o servidores, independientemente del tiempo que permanezcan alejados.
- Las estaciones de trabajo y terminales no deben estar activas cuando sean desatendidas y deben ser protegidas mediante uso de contraseñas u otros controles cuando no estén siendo utilizadas.
- Se debe establecer un método de bloqueo (contraseñas, patrones, etc.) para los equipos que serán entregados a los usuarios, y que se bloquee pasado un tiempo no mayor a cinco minutos de inactividad.
- Al terminar la jornada de trabajo se deberá apagar el equipo, siempre y cuando no se encuentren ejecutándose procesos programados fuera de horario de oficina y respondan a labores propias del cargo del trabajador. En caso de ausentarse de la oficina por un período prolongado de tiempo, se deberán cancelar las sesiones de usuario dentro de las aplicaciones, además de bloquear la pantalla.
- Todo usuario debe desconectarse de las aplicaciones o de servicios de red cuando ya no sea necesario.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA USUARIOS

Política de Escritorio Limpio

- Es responsabilidad de todo colaborador mantener sus escritorios o puestos de trabajo limpios y sin documentos fuera del horario de trabajo o en ausencia prolongada del sitio para evitar el acceso no autorizado o fuga de información.
- Se debe evitar exponer información confidencial e interna en los módulos, escritorios o estaciones de trabajo de la empresa.
- El colaborador o proveedor no deberá tener escrito en un medio físico (papel adhesivo, papel convencional, superficies, etc.) su cuenta de red, credenciales de acceso de correo electrónico, aplicación, sistema de información, datos personales o información relevante que comprometa la seguridad de la información.
- Al ausentarse del puesto de trabajo se deberá guardar en un lugar seguro información física o medios removibles que contengan información confidencial o sensible.
- Los documentos digitales enviados a impresión, se deberá recoger inmediatamente, toda vez que esta sea considerada como confidencial o sensible.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA USUARIOS

- No se arrojará al tacho de basura, documentos impresos que contengan información confidencial o sensible. Antes deben ser destruidos de forma irrecuperable.

Política de Pantalla Limpia

- No se deberá almacenar en la pantalla del escritorio de la estación de trabajo, información digital conteniendo credenciales personales o corporativas o información confidencial que pueda comprometer la seguridad de la información.
- Se deberá mantener el escritorio del sistema operativo libre de archivos o iconos que saturen y confieran una práctica de almacenamiento riesgosa.
- Los archivos que contengan información confidencial o sensible deben ser guardados en un repositorio de red que cuente con seguridad de acceso y respaldo.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA USUARIOS

Política de Teletrabajo/Trabajo Remoto

- Todas las políticas presentes son aplicables en trabajo remoto.
- El colaborador debe establecer un ambiente de trabajo adecuado para el desarrollo de sus actividades (considerar ergonomía, iluminación, entre otros).
- En la medida de lo posible, configurar el router con una contraseña segura.
- Resguardar en cajones o gavetas con llave los documentos físicos y medios de almacenamiento que contengan información clasificada como confidencial o restringida.
- En la medida de lo posible, evitar que personas no autorizadas accedan a tu estación de trabajo.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA USUARIOS

Política de WIFI

- No se brinda las contraseñas de Wifi de la empresa a ningún colaborador/ visitante.
- En caso de solicitudes especiales, estas deben ser comunicadas y aprobadas por el Gerente General/ OSI/ Gerente de administración/ Gerente de Soluciones de Tecnología.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA USUARIOS

Política de Uso de Correo Electrónico

- No utilizar el correo electrónico institucional para temas personales, mantener el uso del correo institucional para los fines adecuados.
- Cuidar siempre la ortografía y gramática, tomar en cuenta que representamos a la empresa.
- Utilizar siempre un lenguaje cordial y educado.
- No abrir adjuntos/ links de remitentes desconocidos o sospechosos, reportar siempre estos casos a segurinfo@consejeros.com.pe
- No responder ni reenviar correos sospechosos (cadenas de mensajes, publicidad, sorteos, etc.) lo más probable es que se traten de un virus.
- No reenviar mensajes sin el permiso del remitente, sobre todo aquellos con contenido confidencial.
- Asegurarse de que la firma esté correctamente configurada.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA USUARIOS

Política de Navegación Web

- El acceso a internet debe ser solo de interés laboral y no personal.
- Todos los usuarios deben seguir los principios corporativos con respecto al uso de los recursos y ejercer buen juicio sobre el uso de internet.
- El uso aceptable de internet incluye el soporte técnico de TI para descargar actualizaciones y parches de software.
- El uso aceptable de internet incluye temas de investigación y búsqueda de temas que ayuden con la realización de las tareas asignadas por la empresa.
- Se tiene bloqueado el acceso a páginas con temas de contenido para adultos, redes sociales, juegos online, páginas de música y videos y otros contenidos inapropiados.
- Se debe mantener en todo momento la confidencialidad de sus datos de acceso a internet, siendo el usuario el único responsable del buen o mal uso de sus datos de acceso.
- Se debe notificar de manera inmediata al área de Soluciones de Tecnología cualquier uso no autorizado de su cuenta o cualquier otra observación de seguridad.
- Sólo se deben manejar correos electrónicoss institucionales.
- Se deben usar sitios web oficialmente permitidos (https).

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA USUARIOS

Acciones Prohibidas

- Divulgar información confidencial o sensible.
- Acceder a internet con fines comerciales o recreativos (juegos, páginas de música y videos, etc.)
- Tener bebidas o comidas cerca de los equipos informáticos que puedan dañar su funcionamiento, siendo el usuario responsable por el deterioro del mismo.
- Intentar acceder a recursos sin autorización, mediante la utilización de herramientas intrusivas (hacking), descifre de contraseñas, descubrimiento de vulnerabilidades o cualquier otro medio no permitido.
- Intentar cargar archivos que contengan virus, archivos dañados, etc., que pueda dañar el funcionamiento de los equipos de la red.
- Enviar correos basura, spam o cadenas de promociones, etc., no autorizado previamente por los usuarios.
- Suplantar la identidad de otro usuario o entidad, engañar o confundir sobre el origen de las comunicaciones u otro contenido.
- Cualquier actividad que intente la recopilación de información de cualquier tipo o sistema con propósitos no acordados previamente.
- Descargar software de internet en cualquier equipo.
- Compartir contraseñas, realizar acciones con el usuario de otra persona; el colaborador es responsable de su usuario y las acciones realizadas con este.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA USUARIOS

Incumplimiento de las Políticas

El incumplimiento de estas políticas de seguridad de la información traerá consigo las consecuencias legales que apliquen a la normativa y proceso disciplinario de la empresa.

Consejeros se reserva el derecho de evaluar periódicamente el cumplimiento de este reglamento.

POLÍTICA DE SEGURIDAD DE INFORMACIÓN PARA LA RELACIÓN CON LOS PROVEEDORES

Política de Seguridad de Información Para la Relación Con los Proveedores

- El proveedor deberá firmar y entregar el documento la constancia de recepción de la presente política de seguridad de la información para las relaciones con los proveedores antes de iniciar el trabajo.
- Todo proveedor que tenga acceso a la información, se asegurará que su personal que formará parte del servicio lea, entienda y cumpla la presente política.
- Todo proveedor proporcionará los datos completos de la persona de contacto, quien será el encargado de recibir todo tipo de directivas de seguridad de la información.
- El proveedor deberá cumplir los siguientes puntos respecto a su personal:
  - Verificar los antecedentes profesionales, penales y policiales del personal que forma parte del servicio, a fin de garantizar a la institución que no exista ningún tipo de sanción aplicado en la actualidad.
  - Concientizar y/o capacitar cuando se requiera en temas relaciones a seguridad de la información.

POLÍTICA DE SEGURIDAD DE INFORMACIÓN PARA LA RELACIÓN CON LOS PROVEEDORES

- En el caso de que se realice cualquier cambio en el personal como baja, sustitución o cambio de funciones o responsabilidades el proveedor deberá informar a la institución para que se tomen las medidas o se inicie el procedimiento correspondiente. Si el cambio es aprobado y se realiza, el proveedor se asegura que se cumpla con el punto 1 y 2.
- El proveedor se asegurará que solo se realicen las actividades que están mencionadas en el contrato y/o términos de referencia correspondiente al servicio prestado. Además, debe garantizar el cumplimiento del contrato y en algunos casos los acuerdos de niveles de servicio que formen parte del servicio prestado.
- Todo proveedor deberá velar que el personal que presta los servicios directamente a la organización, cumpla con los lineamientos establecidos en la presente política. En caso de incumplimiento, la organización se reserva el derecho de solicitar al proveedor el cambio de personal, sin perjuicio del derecho de la institución de resolver el contrato de prestación de servicios en los términos establecidos en el contrato o términos de referencia.

POLÍTICA DE SEGURIDAD DE INFORMACIÓN PARA LA RELACIÓN CON LOS PROVEEDORES

- El proveedor garantizará que todo intercambio de información con CONSEJEROS durante la ejecución del servicio tendrá carácter confidencialidad y no podrá ser utilizada ni manipulada fuera del marco establecido en el contrato de prestación de servicios.
- El proveedor deberá garantizar que todo su personal que realiza servicios para la institución cuente con formación y capacitación apropiada para el desarrollo del servicio contratado, tanto a nivel específico en las materias correspondiente a la actividad asociada, como de manera transversal en materia de seguridad de la información.
- En el caso de que el proveedor conozca de cualquier pérdida, uso no autorizado, revelación de la información proporcionada o de propiedad de la institución o cualquier otro evento/debilidad/incidente de seguridad de la información, deberá comunicarlo inmediatamente a través de los canales de seguridad de la información proporcionados, y en caso que fuera necesario debiendo adoptar todos los pasos necesarios para ayudar a la entidad a remediar tal uso no autorizado o revelación de la información.
- El proveedor deberá garantizar que todos los recursos que la organización le proporcione sean utilizados únicamente para cumplir con las actividades del servicio prestado.

POLÍTICA DE SEGURIDAD DE INFORMACIÓN PARA LA RELACIÓN CON LOS PROVEEDORES

- Todo proveedor deberá de tener en cuenta que la información de la organización no debe ser utilizada para beneficio propio o de terceros y solo deberá ser utilizada para los fines establecidos en el contrato de prestación de servicios.
- Todo proveedor es responsable de transmitir y hacer cumplir la presente política a terceros subcontratados, autorizados debidamente por la organización.
- El proveedor deberá garantizar que toda información que fue recibida durante la ejecución del servicio prestado deberá ser eliminada de su poder al finalizar el servicio.
- Todo proveedor se asegurará de cumplir todas las obligaciones de confidencialidad aún culminado el contratado de prestación de servicios por cualquier motivo.
- Los terceros deberán registrar al momento de su entrada, en el control de ingreso, el ingreso de equipos de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de CONSEJEROS.

POLÍTICA DE SEGURIDAD DE INFORMACIÓN PARA LA RELACIÓN CON LOS PROVEEDORES

- El servicio entregado por terceros según su criticidad e impacto en la continuidad del negocio, deberán incluir parámetros de seguridad de información dentro del contrato establecido con CONSEJEROS o del acuerdo de nivel de servicio (sla – service level agreement), de ser el caso y contemplar penalidades ante el incumplimiento.
- El nivel de servicio de los terceros respecto a temas de tecnología debe ser evaluado y aceptado por la oficina de Soluciones de Tecnología de la información, con opinión previa de seguridad de información (de corresponder).
- En el caso que el servicio incluya la creación de una cuenta de correo electrónico de la institución, está debe ser usada para el desempeño de las funciones asignadas dentro de la institución.
- Los administradores de servidores, bases de datos y demás roles que manejen información clasificada como confidencial, deben garantizar la confidencialidad de la información y el uso de credenciales de administración (usuario y contraseña), sin excepción.

POLÍTICA DE SEGURIDAD DE INFORMACIÓN PARA LA RELACIÓN CON LOS PROVEEDORES

- El servicio de acceso remoto deberá permitir el acceso a la red de datos a aquellos usuarios externos expresamente autorizados por el usuario del servicio y el Oficial de seguridad de la información, para que lo hagan desde redes externas o internas, el cual debe estar sujeto a autenticación con un nivel adecuado de protección y obedecer a necesidades justificadas.
- No se debe proveer información sobre la ubicación del centro de procesamiento de datos o de los lugares críticos, como mecanismo de seguridad.
- El proveedor deberá garantizar que el servicio prestado puede ser periódicamente monitoreado para verificar su cumplimiento.

OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

1. Proteger la confidencialidad de la información, asegurando que sea accesible a los usuarios, colaboradores y terceros con una legítima necesidad de saber.
2. Monitorear la asignación de accesos y permisos a los sistemas internos y externos.
3. Salvaguardar la integridad de la información para garantizar su exactitud y totalidad.
4. Mantener y asegurar la disponibilidad de la información y los sistemas de información que soportan los procesos de Consejeros para garantizar que los colaboradores, proveedores, entidades y usuarios autorizados tengan acceso a la información cuando lo requieran.
5. Monitorear los riesgos de seguridad de la información para mantenerlos en niveles aceptables.
6. Comunicar y registrar oportunamente la ocurrencia de eventos, debilidades e incidentes que afecten la seguridad de la información con el fin de evitar que vuelva a ocurrir.
7. Mantener constante vigilancia y registro de los posibles incidentes y actividades sospechosas de forma que podamos prevenir eventos no deseados.
8. Fortalecer la cultura de seguridad de la información en los colaboradores, contratistas, proveedores y usuarios de la organización. Promover la capacitación del personal, cumpliendo con las capacitaciones planificadas anualmente.
9. Monitorear la eficacia para la mejora continua del SGSI y cumplimiento de los requisitos legales, contractuales, normativos y/o regulatorios que afectan a la organización en temas de seguridad de la información.
10. Monitorear los hallazgos encontrados en auditorías anteriores para la mejora continua del SGSI, con la finalidad de asegurarse que han sido subsanados y procurar que no vuelvan a repetirse.
11. Monitorear oportunamente las cláusulas de los acuerdos contractuales del SGSI, ante incumplimiento de la política de seguridad de la información.

ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

En concordancia con la distribución de personas y actividades, a continuación, se indican las funciones y responsabilidades de los involucrados en el SGSI.

Representante de la Alta Dirección – Gerente General

- Brindar su apoyo y compromiso con el SGSI.
- Designar, integrar y liderar al Comité de Gestión de Seguridad de la Información.
- Asegurar la disponibilidad de los recursos (humanos, de infraestructura, financieros y tecnológicos) para los proyectos relacionados con el SGSI.
- Aprobar la política y objetivos de seguridad de la información, así como velar por su publicación y distribución.
- Asegurar que se establezca y mantenga el SGSI de acuerdo a la ISO/IEC 27001:2022.
- Dirigir y coordinar el avance y eficacia del SGSI en función a resultados de objetivos, metas y auditorías internas.

ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

- Apoyar activamente en el cumplimiento y mejora continua del SGSI.
- Asegurar que exista un marco de trabajo adecuado para identificar, medir, monitorear y reportar los riesgos de seguridad de la información de la empresa.
- Difundir la importancia de una efectiva gestión de seguridad de la información a las partes interesadas, en conformidad con los requisitos del SGSI.
- Definir las funciones, asignar responsabilidades y delegar autoridad y responsabilidad a cada una de las áreas para el cumplimiento de la política y objetivos de seguridad de la información.

Comité de Gestión de Seguridad de la Información

- Revisar que la política y objetivos de seguridad de la información se encuentren alineados con los objetivos estratégicos de la organización y regulación en el ámbito de seguridad de la información.
- Promover y gestionar la implementación, mantenimiento y mejora del SGSI.

ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

- Evaluar los resultados del desempeño del SGSI.
- Decidir el criterio para la aceptación de riesgos de seguridad de la información y los niveles de riesgo aceptables.
- Otras funciones que se le asigne en el ámbito de su competencia y aquellas concordancias con la materia.

Oficial de Seguridad de la Información

- Dirigir, coordinar y controlar todas las actividades relacionadas con el SGSI.
- Liderar y velar por el desarrollo, implementación, mantenimiento y cumplimiento de políticas y procedimientos para promover la seguridad de la información.
- Informar al GG y CGSI sobre el desempeño del SGSI, para su revisión y como base para el mejoramiento de este sistema de gestión.
- Coordinar y proponer la agenda de las sesiones del CGSI, registrar en actas lo actuado y los acuerdos tomados en las sesiones por el CGSI; y custodiar los registros.

ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

- Liderar la realización de actividades orientadas al análisis, evaluación y tratamiento de riesgos y oportunidades de seguridad de la información periódicos, a fin de mantener un conocimiento actualizado de las amenazas y vulnerabilidades.
- Liderar el proceso de gestión de incidentes de seguridad de la información.
    - Registrar todos los eventos, debilidades e incidentes reportados.
    - Analizar los eventos, debilidades e incidentes reportados.
    - Evaluar y tomar una decisión sobre los incidentes reportados.
    - Planificar y preparar una respuesta sobre el incidente.
    - Hacer seguimiento a los incidentes reportados y respuesta.
    - Verificar que se cumpla con lo estipulado en los procedimientos vigentes.
- Monitorear la efectividad de los controles implementados para la protección de los activos de información.
- Promover la difusión y apoyo a la seguridad de la información dentro de la organización.

ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

- Proponer, ejecutar los planes y programas de concientización en materia de seguridad de la información y, capacitar en forma constante y continua a todo el personal relacionado con la seguridad de la información de la organización.
- Asesorar a las distintas áreas de la organización en temas relacionados a seguridad de la información.
- Apoyar en la revisión gerencial del SGSI y necesidades de mejora.
- Apoyar en la planificación y realización de las auditorias del SGSI.
- Realizar el seguimiento de las acciones correctivas.
- Promover y hacer seguimiento de la mejora continua.
- Elaborar y cuando corresponda revisar, los documentos referidos a la seguridad de la información.
- Monitorear cambios significativos en la infraestructura que puedan poner en riesgo los activos de información de la organización.
- Otras funciones que le asigne el GG o el CGSI en el ámbito de sus competencias y aquellas concordantes con la seguridad de la información.

ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

Propietario de riesgos

- Participar y/o delegar al personal que participará en las actividades de identificación, análisis, evaluación y tratamiento de los riesgos de seguridad de la información.
- Evaluar y aceptar el riesgo residual de seguridad del activo de información, y revisarlos periódicamente; así como los criterios de evaluación y aceptación de riesgos.
- Aprobar el plan de tratamiento de riesgos y contribuir a la implementación de los controles de seguridad de la información que estén relacionados a sus responsabilidades.
- Brindar información oportuna y pertinente para la elaboración de indicadores y métricas, auditoría, revisión y mejora continua del SGSI, cuando sea requerido.

ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

Propietario de oportunidades

- Participar y/o delegar al personal que participará en las actividades de identificación, análisis, evaluación y tratamiento de las oportunidades.
- Aprobar el plan de tratamiento de oportunidades y contribuir a la implementación de las acciones a fin de que las oportunidades se materialicen.
- Brindar información oportuna y pertinente para la elaboración de indicadores y métricas, auditoría, revisión y mejora continua del SGSI, cuando sea requerido.

Propietario de activo de información

- Participar en los procesos de identificación, clasificación y valoración de activos de información.
- Autorizar la asignación de accesos sobre la información.
- Autorizar los cambios sobre los activos de información de su propiedad.

ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

- Apoyar activamente en las actividades de identificación, análisis, evaluación y tratamiento de los riesgos de seguridad de la información.

Gerentes y/o Jefes

- Apoyar en la difusión de las políticas y procedimiento de seguridad de la información de la organización al personal bajo su cargo.
- Comunicar requerimientos de control y protección de la información al OSI y asegurar que la información y recursos bajo su control estén debidamente protegidos por las medidas de seguridad adecuadas.
- Apoyar y facilitar las revisiones periódicas para la verificación del cumplimiento de las políticas y procedimientos de seguridad de la información.
- Determinar los criterios y niveles de acceso a la información de la cual son responsables y notificar el cambio de función/ubicación de cualquier personal de la organización sea por reasignación o retiro, con la finalidad de modificar o cancelar sus accesos.

ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

- Reportar el incumplimiento o infracciones a las políticas y normas de seguridad.
- Aprobar y/o revisar todos los procedimientos y formatos del SGSI que le correspondan.
- De ser el caso, con respecto a observaciones, no conformidad u oportunidades de mejora, producto de auditorías, acciones correctivas, revisiones por la dirección u otros:
  - Aprobar el plan de acción para la atención de la no conformidad, observación u oportunidad de mejora.
  - Gestionar las acciones correctivas o de mejora bajo su responsabilidad.
  - Reportar al OSI, los avances en la realización de las acciones correctivas o de mejora, cuando sea requerido.

Personal de la empresa

- Conocer, comprender y cumplir las políticas y procedimientos de seguridad de la información de la organización.

ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

- Identificar y notificar debilidades, eventos, incidentes y riesgos de seguridad de la información al jefe inmediato superior y/o al OSI.
- Apoyar en las actividades relacionadas a la gestión de riesgos de seguridad de la información.
- Utilizar la información, sistemas y todos los recursos de la organización únicamente para los propósitos autorizados e inherentes a la función asignada.
- Mantener la confidencialidad e integridad de la información durante y después del vínculo laboral con la empresa.
- Reportar incumplimientos (no conformidad, observación) u oportunidades de mejora detectados en seguridad de la información.
- Participar en las charlas de concientización o capacitaciones en seguridad de la información.

ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

Terceros o proveedores

- Cumplir las políticas de seguridad de la información que les aplique, las cláusulas incluidas dentro de los contratos o el acuerdo de confidencialidad, que están referidas a salvaguardar la confidencialidad, integridad y disponibilidad de la información de la organización.
- Brindar todas las facilidades necesarias para que la organización revise el cumplimiento de las condiciones incluidas en los contratos de los servicios brindados; así como también aspectos de seguridad de la información de los servicios.
- Identificar y notificar debilidades, eventos, incidentes y riesgos de seguridad de la información al área usuaria que lo contrato y/o al OSI.

Consejeros

CORREDORES DE SEGUROS

Lima - (01) 200 4 200

Arequipa - (054) 38 0303

Tacna - (052) 42 8282

www.consejeros.com.pe

segurinfo@consejeros.com.pe *

** Dirección de correo electrónico para reportar observaciones y/o incidentes relacionados a la Seguridad de la Información de la empresa.*