POLÍTICA DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

ENERO 2021

	POLÍTICA DEL SISTEMA DE GESTIÓN DE SEFLURIDAD DE LA INFORMACIÓN		
	Elaborado	**Revisa**	**Aprueba**
Nombre	Bryan Rivera	Luis Sairitupa	Luis Sairitupa
Cargo	Control & Compliance Coordinator	CEO	CEO
Fecha	31/12/2020	03/01/2021	03/01/2021
Uso de Inf.	Interno		
Código	POL – SGSI - 002		

I. ASPECTOS GENERALES

OBJETIVO

El Objetivo de esta Política de Seguridad del SGSI es proteger la confidencialidad, integridad, disponibilidad de los activos de información mediante una adecuada gestión de riesgos; conforme con los requisitos legales, reglamentarios y las obligaciones adquiridas contractualmente por Imperia Soluciones Tecnológicas S.A.C en adelante IMPERIA.

ALCANCE

Esta Política es aplicable a todos los trabajadores y terceros, que usen los recursos de información que sean propiedad de IMPERIA.

MARCO DE REFERENCIA

ISO/IEC 27001:2022

DOCUMENTOS RELACIONADOS

NO APLICA

TÉRMINOS Y DEFINICIONES

- **Confidencialidad:** propiedad de la información por la que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** propiedad de exactitud y completitud.
- **Disponibilidad:** propiedad de ser accesible y estar listo para su uso a demanda por una entidad autorizada.
- **Mejora continua:** actividad recurrente para mejorar el desempeño.
- **Dato Personal:** Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados.
- **Datos sensibles:** Es aquella información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten su intimidad

II. POLÍTICA GENERAL

La Alta Dirección reconoce a la información y los sistemas que la sustentan y procesan como uno de sus activos más importantes a proteger, y establece como objetivo la gestión adecuada de los riesgos relacionados.

La Alta Dirección asume la responsabilidad de promover y apoyar el establecimiento de medidas técnicas, organizativas y de control que garanticen la integridad, disponibilidad y confidencialidad de la información, dentro de un marco general de gestión de riesgos de seguridad.

VIGENCIA

Lo dispuesto en la presente política es de uso obligatorio, y entrará en vigor a partir de la fecha de su aprobación, permaneciendo vigente hasta la aprobación y/o publicación de otro documento de similar jerarquía que lo sustituya.

COMUNICACIÓN DE LA POLÍTICA

Se debe asegurar que la política es comunicada, entendida e implementada en toda la organización y debe ser de conocimiento de los trabajadores y demás partes interesadas.

MEJORA CONTINUA

La Política de Seguridad de la Información será revisada por lo menos una vez al año o si ocurren cambios significativos para garantizar su idoneidad, adecuación y efectividad continua.

REQUISITOS LEGALES

Se deben de cumplir todos los requisitos legales establecidos en el documento Listado de Legislación Aplicable aprobado por el Comité SGSI.

GESTIÓN DE RIESGOS

Se dispone de criterios para la gestión de riesgos aprobados para identificar, cuantificar, priorizar y tratar los riesgos de Seguridad de la Información a fin de poder establecer los controles apropiados para los riesgos identificados que entren al plan de tratamiento de riesgos.

La evaluación de riesgos debe realizarse como mínimo una vez al año y cada vez que se identifiquen cambios significativos dentro de la organización, debiendo asegurarse de que son monitoreados y se realiza el seguimiento para medir la efectividad de los controles implementados.

RESPONSABILIDADES

RESPONSABILIDADES DE LAS GERENCIAS Y ÁREAS

- Realizar y participar en las actividades y acciones que permitan mantener el Plan de Seguridad de la Información vigente y con los controles adecuados.
- Participar en los equipos de trabajo, actividades y acciones relacionadas a Seguridad de la Información.

RESPONSABILIDADES DE LOS TRABAJADORES

- Conocer y cumplir con lo establecido en la Política de Seguridad de la información aprobada y vigente.
- Notificar los incidentes de seguridad de la información conforme a los canales de comunicación establecidos.
- Guardar secreto y mantener la confidencialidad sobre toda la información y datos de carácter personal y de terceros a los que tenga acceso en virtud de su trabajo, obligación que subsistirá incluso después de finalizar su relación con la organización.

III.SANCIONES POR INCUMPLIMIENTO

- **IMPERIA** se reserva el derecho de tomar medidas disciplinarias con los trabajadores que incumplan con lo dispuesto en la Política de Seguridad de la Información, conforme a las disposiciones señaladas en los documentos normativos de la organización, sin prejuicio de las acciones civiles y/o penales que pudieran corresponder.

- Asimismo, si se comprueba que un colaborador ha accedido, modificado, eliminado, substraído o perdido información a la que no estuvo autorizado podrá suponer causa suficiente de apertura de proceso disciplinario, conforme a la tabla que se muestra a continuación:

CLASIFICACION DE LA INFORMACIÓN	SANCION POR INCUMPLIMIENTO
Confidencial	Si se demuestra que un colaborador ha modificado, eliminado, sustraído o extraviado información confidencial se abrirá proceso y se le retirarán los privilegios de acceso. Investigada la causa, se determinará si corresponde la suspensión temporal o despido considerando lo dispuesto en la normatividad vigente que establece las causas justificadas de despido.
Uso Interno	Si un colaborador hace un mal uso de información de uso interno de la que carece de privilegios, se le dará un aviso de advertencia y se tendrá en cuenta en su evaluación de desempeño.
Pública	No existe un proceso disciplinario con respecto a este tipo de Información.

SEGURIDAD DE LA INFORMACIÓN EN GESTIÓN DE PROYECTOS

- Se debe integrar la seguridad de la información en los métodos de gestión de proyectos de la organización para asegurarse de que se identifican y tratan los riesgos de seguridad de la información como parte de los proyectos, es decir, los riesgos asociados a la perdida de Confidencialidad, Integridad y Disponibilidad. Esto se aplica a cualquier proyecto, sin importar su carácter. Para la gestión de riesgos se utilizará los criterios aprobados dentro de la Organización.

SEGURIDAD EN DISPOSITIVOS MÓVILES

- Los trabajadores de **IMPERIA** son responsables de la confidencialidad, integridad y disponibilidad de la información contenida en los equipos móviles asignados, especialmente cuando se encuentren fuera de las dependencias de la organización.
- Los trabajadores no deben almacenar en el equipo móvil, información confidencial de la organización.
- En caso de pérdida del computador portátil o teléfono móvil, el incidente deberá ser comunicado inmediatamente a su jefe directo y el Oficial de Seguridad.

SEGURIDAD DE RECURSOS HUMANOS

- Se debe integrar la seguridad de la información en todas las etapas de selección de personal, durante el empleo y al finalizar el mismo.
- La Organización debe asegurar que los trabajadores y proveedores comprendan sus responsabilidades y que sean adecuados para los roles en los que se les ha considerado.
- Se debe asegurar que los trabajadores reciban educación y capacitación de concienciación sobre seguridad de la información.
- Se planificará anualmente las actividades de capacitación y concienciación en Seguridad de la Información para los trabajadores con la finalidad de crear una cultura sobre Seguridad de la Información que logre reducir las brechas de exposición de riesgos.

PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

- Todo tratamiento de datos personales o datos sensibles será previo consentimiento libre, previo, expreso e informado de su titular.
- Se deben establecer los términos, condiciones y finalidades del tratamiento de datos personales conforme a lo establecido en la Ley de Protección de Datos Personales y su Reglamento.
- Los trabajadores de **IMPERIA** deben guardar secreto y mantener la confidencialidad sobre toda la información y datos de carácter personal a los que tenga acceso en virtud de su trabajo, obligación que subsistirá incluso después de finalizar su relación con la organización.
- Los trabajadores de **IMPERIA** tienen acceso únicamente a información que han sido autorizados para el desarrollo de sus funciones en función de su cargo o responsabilidades.
- Para el caso de los datos personales y/o sensibles trabajadores de **IMPERIA** la organización se compromete a preservar confidencialidad e integridad de la información que conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la organización y no sea publicada, revelada o entregada a personas o terceras partes sin autorización expresa del titular de los datos.
- Se deben de implementar los controles necesarios para proteger la información personal de sus clientes, trabajadores, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio a fin evitar su divulgación, alteración o eliminación sin la autorización expresa requerida del titular de los datos.
- Queda terminantemente prohibido hacer entrega, por cualquier medio y sin autorización, de listados o de bases de datos a personas no autorizadas, ya sea de forma total o parcial.
- Los titulares de datos personales podrán ejercer en cualquier momento sus derechos de información, acceso, rectificación, cancelación y oposición por medios de los procedimientos establecidos en la organización.

GESTIÓN DE ACTIVOS

Se debe identificar los activos asociados a la información y a los recursos para tratamiento de la información y ser registrados en un inventario. El inventario será actualizado ante cualquier modificación de la información registrada y revisado periódicamente.

Todos los activos deben tener un propietario. El propietario de cada activo debe asegurase que la clasificación de la información sea adecuada y revisar periódicamente su clasificación.

Propietario de la Información

- Clasificar la Información de su propiedad.
- Definir si el activo está afectado por la Ley de Protección de datos personales.
- Definir quién, cómo y cuándo se puede tener acceso a la información.
- Asegurarse de que el activo cuenta con el manejo adecuado cuando se elimine o destruya.
- Autorizar la desclasificación de la Información de su propiedad.
- Gestionar la rotulación correspondiente a la Información de su propiedad.
- Para Información de su propiedad que tenga una clasificación distinta de Pública:
  - Evaluar y autorizar la divulgación.
  - Evaluar y autorizar la reproducción.
  - Autorizar el acceso.

El propietario de la información es responsable de validar a intervalos planificados que para la información Confidencial y de uso interno se apliquen los controles de seguridad adecuados y solo acceda el personal autorizado durante todo su ciclo de vida.

Custodio de información

- Clasificar y proteger la información, de acuerdo a lo definido por el propietario de esa información.

- Con respecto a los equipos de cómputo asignados a los trabajadores para el desarrollo de sus labores, se prohíbe bajo responsabilidad que se instale software que no sea proporcionado por **IMPERIA**. En caso de requerir algún software adicional deberá solicitarlo al personal autorizado de Soporte Técnico utilizando los canales de comunicación establecidos.
- Cuando algún colaborador deje de laborar en la organización, debe de devolver todos los activos de información (físicos y lógicos) a su jefe inmediato superior; para el caso de los equipos y dispositivos puestos a su disposición serán devueltos personal autorizado de Soporte Técnico.

CLASIFICACIÓN, TRATAMIENTO Y CONSERVACIÓN DE LA INFORMACIÓN

IMPERIA ha establecido una clasificación para la información la misma que puede ser tratada como confidencial, uso interno o público, conforme lo establecido a continuación:

Tipo	Descripción
Confidencial	Se refiere a la información de uso exclusivo y restringido a un grupo de trabajadores de **IMPERIA**. Incluye datos personales, datos sensibles e información cuya divulgación puede impactar a la empresa, terceros o clientes.
Uso Interno	Aquella información de uso interno y exclusivo de todas las gerencias de **IMPERIA**. Para que un personal no perteneciente a Imperia pueda acceder a esta información se requiere la firma de acuerdos de confidencialidad siempre y cuando su divulgación no afecte a la empresa, terceros y clientes.
Publica	Es la información que, por su naturaleza, no representa ningún riesgo para **IMPERIA** y que pueda ser dada a conocer al público en general.

- Para el tratamiento de la información los trabajadores deben considerar la clasificación asignada a la información para establecer los niveles de protección adecuados.
- Se debe etiquetar la información de acuerdo con el esquema de clasificación de información adoptado por la organización. En caso la información no se haya etiquetado, se considerará su clasificación por defecto de uso interno
- Se debe conservar la información conforme a los requisitos legales, regulatorios o contractuales.
- Para los medios extraíbles se deben adoptar controles de acuerdo con el esquema de clasificación de la información adoptado en la organización.
- Para los medios que contienen información confidencial se deben almacenar de manera segura, implementando medidas de seguridad que eviten el acceso, manipulación y divulgación no autorizada.
- Para los medios físicos que contengan información en tránsito se debe de usar transportes o mensajeros confiables.
- Toda información en papel o contenida en dispositivos de almacenamiento que contengan información clasificada como confidencial, y se desee eliminar, debe contar con autorización del propietario y debe ser destruida de modo que sea imposible su recuperación.

CONTROL DE ACCESOS A LOS RECURSOS DE INFORMACIÓN

- Todos los accesos a los recursos de información de **IMPERIA** deben tomar en cuenta los siguientes aspectos:

a) Acceso basado en Roles o Perfiles de usuario (necesidad de conocer).
b) Los requerimientos de seguridad de cada una de las aplicaciones considerando siempre el principio de menor privilegio.
c) Identificación de toda la información relacionada a las aplicaciones y los riesgos a la que está expuesta.

d) Legislación pertinente y cualquier tipo de obligación contractual con respecto a la limitación de acceso a los datos o servicios.
e) Uso de perfiles de usuarios estandarizados definidos según perfil de puesto.
f) Requisitos para la autorización formal de las solicitudes de acceso.
g) Revisión periódica de los controles de acceso.
h) Revocación de los derechos de acceso.
i) Gestión de derechos de acceso privilegiado.

- El acceso a la red y sistemas de información es controlado mediante políticas de seguridad aplicadas según perfiles de usuario para los trabajadores y personal externo.
- Para el acceso a las distintas aplicaciones internas a los trabajadores de **IMPERIA** se les creará su usuario y contraseña temporal de inicio de sesión considerando su perfil de puesto trabajo.
- Los trabajadores de **IMPERIA** deben sustituir inmediatamente las contraseñas temporales de inicio de sesión entregadas por una contraseña compleja según lo permita la aplicación.
- Las contraseñas de acceso al sistema y aplicaciones deben cambiarse con una periodicidad trimestral y deben ser diferentes y complejas.
- No debe utilizarse las funciones de recordar las contraseñas en ninguno de los sistemas y aplicaciones proporcionados por la organización.
- No debe usarse las contraseñas de la organización para sistemas externos como correos personales, redes sociales, entre otros.
- Las contraseñas son de uso personal e intransferible. Ningún colaborador de la **IMPERIA** podrá solicitar las contraseñas de otros.
- Los trabajadores deben tomar las precauciones para proteger su contraseña. En caso de no recordar la contraseña o se produzca el bloqueo de sesión, deben comunicarlo a Soporte Técnico según los canales establecidos para poder restablecerla.
- En caso los trabajadores tengan alguna sospecha que su contraseña ha sido comprometida o divulgada, deben cambiarla inmediatamente y comunicarlo a Soporte Técnico.
- Las contraseñas no deben estar escritas en soportes de fácil extravío o divulgación.
- Se deben ejecutar revisiones de los derechos de accesos y privilegios en los sistemas y aplicaciones de manera regular, lo que será determinado según la frecuencia de rotación del personal en la organización.

CUENTAS PRIVILEGIADAS

- El acceso privilegiado solo se usa y otorga cuando es necesario, considerando la necesidad de saber, privilegio mínimo, requisitos de privacidad y/o segregación de funciones.
- El uso de múltiple factor de autenticación (MFA) debe ser obligatorio para todas las cuentas con privilegios elevados o de administrador.
- Toda cuenta predeterminada con acceso privilegiado deberá ser deshabilitada, caso contrario se deberá cambiar las credenciales por defecto. Las cuentas privilegiadas solo deben usarse para tareas específicas que requieren permisos elevados.
- Se debe contar con un inventario de cuentas actualizado el mismo que identifique roles y privilegios, este inventario debe considera también las cuentas de servicios si las hubiese; y debe ser revisado de manera semestral.

- Los usuarios con acceso de administrador u otros privilegios deben tener cuentas independientes para esas tareas, asimismo considerar no cuenten con privilegios de usuario para navegar por internet, correo electrónico ni uso de aplicaciones en producción.
- Las cuentas privilegiadas de sistemas y aplicaciones que no permitan integrar MFA o contraseñas complejas deberán renovar en un periodo de 90 días.
- Las cuentas privilegiadas de sistemas y aplicaciones que permitan medidas de seguridad complementaria deberán cambiarse por lo menos una vez al año.

TELETRABAJO

- El Teletrabajo para cualquiera de los trabajadores de Imperia debe estar autorizado.
- El Equipo a utilizar en caso no sea el provisto por IMPERIA debe de contar con Sistema Operativo con licencia y un Antivirus actualizado, para el acceso remoto se utilizará un cliente VPN.
- Para la conexión a internet los trabajadores en ningún caso deben hacerlo desde un sitio de acceso público

USO DE CONTROLES CRIPTOGRÁFICOS

- Los propietarios de activos de información en base a la clasificación de la información dispuesta en la organización y los resultados de la evaluación de riesgos revisarán que los controles implementados sea adecuados, asegurando que la información considerada como Confidencial se le apliquen técnicas de controles criptográficos para lo cual se utilizarán las herramientas de cifrado implementadas en la organización, las mismas que contribuyen a preservar confidencialidad e integridad de la información.
- Se deben establecer lineamientos sobre la generación, el uso, la protección, el cambio y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida.

SEGURIDAD FÍSICA Y AMBIENTAL

- Los perímetros de seguridad están claramente definidos y las medidas de seguridad dependerán del nivel de protección que se requiera lograr.
- Se ha implementado un registro de visitas a las instalaciones de **IMPERIA**.
- Toda persona externa a **IMPERIA** podrá acceder a las áreas restringidas, siempre que cuente con la autorización respectiva y debe estar siempre acompañado por un colaborador.
- Los trabajadores de **IMPERIA** deben portar en todo momento su fotocheck.
- Las instalaciones de procesamiento de información deben estar protegidas adecuadamente y contar con mecanismos de control implementados.
- Las medidas de protección contra amenazas externas y ambientales deben incluir:

a) Controles de acceso y seguridad física.
b) Extintores y/o sistemas de protección contra incendios.
c) Sistemas de acondicionamiento de temperatura, humedad y filtrado de aire.
d) Sistema de alimentación ininterrumpida (UPS).
e) Sistema de aterramiento (pozo a tierra).

- Se debe proteger a los equipos de tecnología de la información de fallas por falta de suministro de energía y otras anomalías eléctricas.

- El cableado de la red de comunicaciones y suministro de energía debe protegerse adecuadamente conforme a estándares internacionales para evitar su intercepción o daño.
- Se debe considerar un programa de mantenimiento preventivo y correctivo de los equipos de tecnología de información y de los sistemas de acondicionamiento de temperatura, humedad y filtrado de aire, sistemas de energía ininterrumpida (UPS) y entres otros según las especificaciones del fabricante. Se debe llevar un registro de los mantenimientos realizados a los equipos de infraestructura de TI.
- Se debe contar con autorización respectiva para el retiro de equipos, de información o software de propiedad de **IMPERIA**.
- Toda documentación (impresa o escrita) de tipo confidencial, así como la información contenida en dispositivos de almacenamiento (CD, DVD, Pendrive, otros) deben ser guardadas en un lugar seguro con llave.
- Los trabajadores que por la naturaleza de sus funciones impriman documentos con información de clasificada como confidencial, deben retirarla inmediatamente de la impresora.
- Los trabajadores no deben almacenar información de tipo confidencial en soportes informáticos no permitidos.
- Toda información en papel o contenida en dispositivos de almacenamiento que contengan información clasificada como de tipo confidencial, y se desee eliminar, debe contar con autorización del propietario y debe ser destruida de modo que sea imposible su recuperación.
- Los trabajadores deben de mantener su puesto de trabajo ordenado y libre de documentación. En caso tengan documentación impresa o en medios de almacenamiento clasificada como confidencial deben de tomar las medidas necesarias para su protección bajo responsabilidad.
- Los trabajadores deben almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
- Los trabajadores deben al finalizar la jornada laboral tener en orden su puesto de trabajo y guarden en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno.
- Los trabajadores no deben de consumir alimentos en los puestos de trabajo, porque pueden originar deterioro de los equipos de cómputo y de la documentación.
- Todas las computadoras deben estar configuradas para bloquearse automáticamente una vez transcurrido los 10 minutos de inactividad.
- Los trabajadores deben bloquear su equipo cada vez que se retiren de su puesto de trabajo de forma manual.

SEGURIDAD EN LAS OPERACIONES Y COMUNICACIONES

- Se deben documentar los procedimientos para la gestión y operación correcta de los recursos o servicios de información.
- Todos los cambios a los recursos de TI deben ser controlados, autorizados registrados y considerar marcha atrás en caso de fallas.
- Se deben controlar los cambios a las instalaciones de procesamiento de información y a los sistemas que afectan a la seguridad de la información.
- Se deben establecer controles de auditoría que permitan contar con registro y supervisión sobre los accesos a los sistemas y aplicaciones los mismos que deben estar protegidos.

- Se debe monitorear, el uso de los recursos para que cumplan con las necesidades actuales y futuras de capacidad y así poder garantizar la disponibilidad y la eficiencia de los sistemas.

PROTECCIÓN CONTRA SOFTWARE MALICIOSO (MALWARE)

- Se debe implementar un conjunto de controles técnicos a nivel de la red, servidores, computadoras y smartphone que permitan la prevención, detección y eliminación de software malicioso.
- Se debe asegurar que todos los servidores, computadoras y smartphone de la organización estén protegidas con un software de protección contra software malicioso con capacidad de actualización automática de firmas.
- Se debe asegurar que el sistema operativo y los aplicativos utilizados en los servidores y computadoras tengan instaladas las últimas actualizaciones de seguridad (parches) con la finalidad de evitar la explotación de vulnerabilidades técnicas.
- Únicamente se podrán instalar, en los servidores y computadoras, las aplicaciones permitidas por la organización; por lo que queda prohibido el uso de software no autorizado.
- Se debe implementar controles en la red para detectar el uso de software no autorizado.
- Se debe implementar controles que eviten o detecten el ingreso a sitios web que se sospecha son de tipo malicioso.
- No abrir correos electrónicos o archivos adjuntos de remitentes desconocidos. No instalar ningún software de complemento en el navegador web.
- Se debe establecer procedimientos para concientizar a los usuarios sobre los peligros ocasionado por software malicioso (malware).
- Se debe disponer de copias de seguridad actualizadas y probadas para restaurar la información en caso de un incidente de software malicioso que secuestre información y pida el pago de un rescate.

RESPALDO Y RECUPERACIÓN DE LA INFORMACIÓN

- Se debe definir la frecuencia de las copias de seguridad y pruebas de restauración de la información considerando su nivel de criticidad para la organización.
- Se deben de realizar como mínimo de 02 copias de seguridad; una de las copias de seguridad debe ser almacenada en un lugar externo a la organización que cuente con controles de seguridad y condiciones adecuadas para su conservación.
- Se deben de realizar pruebas de restauración a las copias de seguridad a fin de asegurar que se pueda obtener correctamente la información almacenada al momento de ser necesaria.

GESTIÓN DE VULNERABILIDADES TÉCNICAS

- Se deben de obtener información sobre los riesgos asociados a las vulnerabilidades técnicas con la finalidad de identificarlos y remediarlos oportunamente implementando medidas adecuadas.
- Se debe tener un inventario de activos actual y completo para adecuada gestión de vulnerabilidades técnicas.
- Se deben definir los recursos de información que se utilizarán para identificar las vulnerabilidades técnicas en base a la lista de inventario de activos y aplicar las actualizaciones de seguridad (parches) según su criticidad a los sistemas vulnerables o la aplicación de otros controles compensatorios.

USO DE LA RED INTERNA, INTERNET Y CORREO

- El uso de los servicios de red y los equipos informáticos es exclusivo para fines laborales.
- El uso de Internet y correo electrónico por parte de los trabajadores queda restringido a fines estrictamente laborales.
- Está terminantemente prohibido utilizar el internet para descargar archivos de ocio, entrar a páginas de radio y televisión en línea, servicios de streaming, entretenimiento, juegos, contenido pornográfico y software sin licencia de uso. Asimismo, el uso del correo electrónico para enviar mensajes que contengan datos de carácter personal o de terceros que puedan vulnerar la privacidad o seguridad de los mismos.
- No se utilizará el correo electrónico para enviar o recibir mensajes con contenidos inapropiados, discriminatorios, difamatorios o dañinos que puedan atentar contra los derechos y libertades de las personas.
- No se debe de abrir correos electrónicos ni descargar documentos adjuntos al mismo, cuyo emisor sea desconocido.
- No se debe adjuntar en los correos electrónicos archivos que superen la capacidad establecida por la organización.
- Todos los trabajadores deben tener especial cuidado en la publicación de fotografías organizacionales (tomadas al interior de la organización), esto debido a que pueden contener información confidencial o de uso interno como cronogramas de proyectos, oportunidades de negocio, entre otras.
- Todos los servicios de tecnología de la información se encuentran sujetos a monitoreo y en caso de detectarse un mal uso de los recursos de parte de los usuarios serán sancionados según lo que corresponda.
- Los trabajadores de **IMPERIA** son completamente responsables de todas las actividades realizadas con sus cuentas de red, correo electrónico y de los sistemas de información asociados a la organización.

REQUISITOS DE SEGURIDAD PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SOFTWARE

- Se debe incluir los requisitos de seguridad en las especificaciones de cualquier sistema a desarrollar o adquirir.
- Se debe de proteger la confidencialidad, autenticidad e integridad de la información en las aplicaciones informáticas de **IMPERIA**.

SEGURIDAD EN RELACIONES CON LOS PROVEEDORES

- Se deben establecer mecanismos de control con proveedores, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos ellos, cumplan con las políticas de seguridad de la información.
- Cualquier cambio en los servicios que preste un proveedor debe ser comunicado, acordado y planificado antes de realizarse.
- Se deben establecer acuerdos con proveedores considerando los requisitos de seguridad de la información que se aplicarán en toda la cadena de suministro para la adquisición de tecnologías, productos o servicios de información y comunicación.

SEGURIDAD EN SERVICIOS DE NUBE

- Antes de seleccionar un servicio en la nube, IMPERIA debe realizar una evaluación del proveedor para asegurar que cumple con los estándares de seguridad de la información de IMPERIA. Esto debe incluir una revisión de las políticas de seguridad del proveedor, así como de su historial de incidentes de seguridad y su capacidad para responder a ellos.
- Se deben implementar políticas de control de acceso rigurosas para los servicios en la nube. Esto incluye la utilización de la autenticación multifactor siempre que el sistema lo permita, la asignación de permisos de acceso en base a la necesidad de conocer, y la revisión regular de los derechos de acceso.
- Los datos almacenados y transmitidos a través de la nube deben ser cifrados en todo momento.
- Se deben implementar las políticas de clasificación y etiquetado de datos para identificar y proteger la información sensible.
- Los servicios en la nube utilizados deben cumplir con todas las leyes y regulaciones pertinentes, incluyendo la ley de protección de datos personales.
- Se debe tener un plan para el respaldo y la recuperación de datos en la nube. Esto incluye la realización regular de copias de seguridad, la comprobación de la integridad de las copias de seguridad, y la realización de pruebas de recuperación.
- Se deben establecer procedimientos para gestionar y notificar cualquier incidente de seguridad que afecte a los servicios en la nube. Esto debe incluir la notificación inmediata a la dirección, al equipo de seguridad, y a cualquier parte afectada, así como la toma de medidas para mitigar y remediar el incidente.
- Se debe realizar un monitoreo continuo de los servicios en la nube para detectar cualquier actividad sospechosa o no autorizada. Además, se deben realizar auditorías regulares para asegurar el cumplimiento de la política y evaluar la eficacia de las medidas de seguridad.

GESTIÓN DE INCIDENTES

- Todos los trabajadores de **IMPERIA** deben reportar los eventos y debilidades que atenten contra la seguridad de la información lo más pronto posible a través de los canales establecidos dentro de la organización.
- Se debe tener procedimiento para reporte y evaluación de eventos y debilidades de seguridad de la información asociados con los recursos o servicios de tecnología de la información.
- Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.
- Se debe tener una base de conocimiento de los incidentes de seguridad de la información y mecanismos que permitan recopilar evidencias de los mismos.
- Los registros de evidencias sobre los incidentes serán almacenados como mínimo por un periodo de tres años y serán parte de la base conocimiento.

CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN

- Se debe determinar los requisitos de seguridad de la información al planificar la continuidad del negocio y la recuperación ante desastres.
- Se debe asegurar la continuidad de las operaciones de seguridad de la información.

- La organización debe verificar los controles de continuidad de seguridad de la información establecidos e implementados en intervalos regulares y poder asegurar que son válidos y eficaces durante situaciones adversas.
- Se debe implementar redundancias en las instalaciones de procesamiento de información para asegurar la disponibilidad de los servicios.

CUMPLIMIENTO

- Todas las legislaciones, regulaciones y requerimientos contractuales deben ser identificadas, documentadas y cumplirse.
- Se deben proteger todos los registros contra pérdidas, destrucción, falsificación, acceso no autorizado y publicación no autorizada de acuerdo con los requisitos legislativos, normativos y contractuales.
- Toda la información debe ser retenida conforme a los requisitos legales, normativos o contractuales.
- Los trabajadores no deben destruir o eliminar registros o información importante, sin la aprobación respectiva de los propietarios de información.
- Se debe respetar los derechos de propiedad intelectual, para lo cual todo el software que se utiliza en la organización debe contar con la respectiva licencia de uso
- Se debe implementar las medidas técnicas, físicas, organizativas y legales que sean necesarias para proteger los bancos de datos personales tratados por la organización, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Se debe realizar las revisiones de la Política de Seguridad y Normas de Seguridad establecidas para evaluar el cumplimiento de las mismas por lo menos una vez al año.
- Se debe considerar revisiones independientes de la seguridad de la información mediante auditorías anuales para asegurar se mantiene de forma eficaz, eficiente y efectiva.
- Se deben realizar revisiones sobre el cumplimiento técnico a la infraestructura TI de la organización para verificar la efectividad de las medidas de seguridad aplicadas acorde a las políticas y normas de seguridad de la información establecidas por lo menos una vez al año.