POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El propósito de la siguiente política es fijar las directrices encaminadas a proteger los datos privados y confidenciales de nuestra empresa, de nuestros empleados y de nuestros clientes, así mismo asegurar que se utilicen correctamente los recursos tecnológicos que la empresa pone a disposición de sus empleados para el desarrollo de sus funciones.

La información incluye datos mantenidos en los sistemas de Seguridad Imperio, en soporte físico (papel), correos electrónicos, registros de llamadas, memorias USB, discos duros y compactos, dispositivos móviles u otros medios de almacenamiento. El tratamiento apropiado de los datos personales es fundamental para ganarse la confianza tanto de nuestros clientes como de nuestros colaboradores.

Esta política es de obligatorio cumplimiento. El funcionario que la incumpla, responderá por sus acciones, omisiones o por los daños causados a la infraestructura de información de la empresa, de conformidad con la normatividad penal vigente y la disciplinaria de la empresa.

Es obligación de todos los empleados atender las siguientes directrices:

Cuentas de Usuarios

- ✓ La solicitud de una nueva cuenta o el cambio de privilegios, deberá hacerse por escrito y ser debidamente autorizada por el Jefe de Medios Tecnológicos.

- ✓ Cuando un usuario recibe una cuenta, debe firmar este documento donde declara conocer las políticas y procedimientos de seguridad de la información y acepta sus responsabilidades con relación al uso de su cuenta.

- ✓ No debe concederse una cuenta a personas que no sean empleados de la empresa, a menos que estén debidamente autorizados por la Gerencia General.

- ✓ El Director Administrativo y financiero debe reportar al Jefe de Medios Tecnológicos sobre los empleados que cesan sus actividades y solicitar la desactivación de su cuenta.

- ✓ No se otorgará cuentas a técnicos de mantenimiento externos, ni permitir su acceso remoto, a menos que el responsable de los sistemas de información determine que es necesario. En todo caso, esta facilidad solo debe habilitarse por el lapso requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto).

- ✓ No se crearán cuentas anónimas o de invitado.

Internet

Internet es una herramienta cuyo uso autoriza la empresa en forma extraordinaria, puesto que contiene ciertos peligros. Los hackers están constantemente intentando hallar nuevas vulnerabilidades que puedan ser explotadas para poder acceder a la información de la empresa.

- ✓ El acceso a internet es únicamente de uso laboral no personal, con el fin de no saturar el ancho de banda y así poder hacer buen uso del servicio.

- ✓ Está prohibido acceder a páginas de entretenimiento, pornografía, de contenido ilícito que atenten contra la dignidad e integridad humana: aquellas que realizan apología del terrorismo, páginas con contenido xenófobo, racista etc. o que estén fuera del contexto laboral.

- ✓ En ningún caso se puede recibir ni compartir información en archivos adjuntos de dudosa procedencia, esto para evitar el ingreso de virus al equipo.

- ✓ Se prohíbe descargar programas, demos, tutoriales, ficheros o documentos que no sean de apoyo para el desarrollo de las tareas diarias de cada empleado y que contravengan las normas de Seguridad Imperio Ltda. sobre instalación de software y propiedad intelectual.

- ✓ Ningún usuario está autorizado para instalar software en su ordenador. El usuario que necesite algún programa específico para desarrollar su actividad laboral, deberá comunicarlo al Jefe de Medios Tecnológicos quien determinará su conveniencia y cotizará a través del proceso de compras, previa autorización de la Gerencia General.

- ✓ Está prohibido instalar programas para ver vídeos, emisoras de televisión y de música vía Internet.

- ✓ Los empleados tendrán acceso solo a la información necesaria para el desarrollo de sus actividades.

Correo electrónico

El correo electrónico es un privilegio y se debe utilizar de forma responsable. Su principal propósito es servir como herramienta para agilizar las comunicaciones que apoyen la gestión de la empresa en el desarrollo de su objeto social.

Es de anotar que el correo electrónico es un instrumento de comunicación de la empresa y los usuarios tienen la responsabilidad de utilizarla de forma eficiente, eficaz, ética y de acuerdo con la ley.

Los usuarios que tienen asignada una cuenta de correo electrónico institucional, deben establecer una contraseña para poder utilizar su cuenta de correo, y esta contraseña la deben mantener en secreto para que su cuenta de correo no pueda ser utilizada por otra persona.

Es obligación del empleado:

- ✓ Utilizar el correo electrónico como una herramienta de trabajo, y no como casilla personal de mensajes, para eso está el correo particular.

- ✓ Evitar enviar archivos de gran tamaño a compañeros de oficina. Si se hace necesario compartir un archivo con estas características deberá publicarlo en la red.

- ✓ Evitar participar en la propagación de mensajes encadenados o en esquemas piramidales o similares.

- ✓ Evitar distribuir mensajes con contenidos impropios y/o lesivos a la moral.

- ✓ Si se recibe un correo de origen desconocido, debe consultar inmediatamente con el Jefe de Medios Tecnológicos sobre su seguridad. Bajo ningún aspecto se debe abrir o ejecutar archivos adjuntos a correos dudosos, ya que podrían contener códigos maliciosos (virus, troyanos, keyloogers, gusanos, etc).

- ✓ Evitar poner "Contestar a todos" cuando se contesta un correo a no ser que este absolutamente seguro que el mensaje puede ser recibido por todos los intervinientes. De igual forma si va a reenviar un correo.

- ✓ Evitar el acceso a las cuentas personales durante la jornada laboral.
- ✓ Cerrar el software de correo electrónico cuando deje de usar su estación de trabajo para evitar que otra persona use su cuenta de correo.
- ✓ Se prohíbe facilitar u ofrecer la cuenta y/o buzón del correo electrónico institucional a terceras personas.
- ✓ Los usuarios que tienen asignada una cuenta de correo electrónico institucional, deben mantener en línea el software de correo electrónico (si lo tiene disponible todo el día), y activada la opción de avisar cuando llegue un nuevo mensaje, o conectarse al correo electrónico con la mayor frecuencia posible para leer sus mensajes.
- ✓ Se debe mantener los mensajes que se desea conservar, agrupándolos por temas en carpetas personales.
- ✓ Utilizar siempre el campo “asunto” a fin de resumir el tema del mensaje. Expresar las ideas completas, con las palabras y signos de puntuación adecuados en el cuerpo del mensaje.
- ✓ Enviar mensajes bien formateados y evitar como norma de cortesía, el uso generalizado de letras mayúsculas.
- ✓ Evitar usar las opciones de confirmación de entrega y lectura, a menos que sea un mensaje muy importante, ya que la mayoría de las veces esto provoca demasiado tráfico en la red.
- ✓ Evitar enviar mensajes a listas globales, a menos que sea un asunto oficial que involucre a toda la institución.
- ✓ El Jefe de Medios Tecnológicos determinará el tamaño máximo que deben tener los mensajes del correo electrónico institucional.
- ✓ Los mensajes tendrán una vigencia no mayor de 30 días desde la fecha de entrega o recepción de los mismos. Superada la fecha de vigencia, los mensajes deberán ser eliminados del servidor de correo.
- ✓ Si se desea mantener un mensaje en forma permanente, éste debe almacenarse en carpetas personales en el disco duro del computador personal.

Computadores, impresoras, periféricos y líneas telefónicas fijas y móviles

- ✓ La infraestructura tecnológica: servidores, computadores, impresoras, UPS, escáner, lectoras y equipos en general; no puede ser utilizado en funciones diferentes a las institucionales.
- ✓ Está prohibido el uso de líneas telefónicas fijas y móviles para comunicación distinta a la relacionada con el trabajo.
- ✓ No se puede instalar ni conectar dispositivos o partes diferentes a las entregadas en los equipos. Es competencia del Jefe de Medios Tecnológicos, el retiro o cambio de partes.
- ✓ Cualquier medio externo de almacenamiento de información traído a la empresa, debe superar una verificación de virus mediante el antivirus instalado, en su defecto, debe ser entregado al Jefe de Medios Tecnológicos para control de circulación de virus.

- ✓ No es permitido destapar o retirar la tapa de los equipos, por personal diferente al Jefe de Medios Tecnológicos o bien a quien designe sin la autorización de este.

- ✓ Los equipos, escáner, impresoras, lectoras y demás dispositivos, no podrán ser trasladados del sitio que se les asignó inicialmente, sin previa autorización del Jefe de Medios Tecnológicos.

- ✓ Se debe garantizar la estabilidad y buen funcionamiento de las instalaciones eléctricas, asegurando que los equipos estén conectados a las instalaciones eléctricas apropiadas de corriente regulada, fase, neutro y polo a tierra.

- ✓ Es estrictamente obligatorio, informar oportunamente al Jefe de Medios Tecnológicos la ocurrencia de novedades por problemas técnicos, eléctricos, de planta física, líneas telefónicas, recurso humano, o cualquiera otra, que altere la correcta funcionalidad de los procesos. El reporte de las novedades debe realizarse tan pronto se presente el problema.

- ✓ Los equipos deben estar ubicados en sitios adecuados, evitando la exposición al sol, al polvo o zonas que generen electricidad estática.

- ✓ Los protectores de pantalla y tapiz de escritorio, serán establecidos por Jefe de Medios Tecnológicos y deben ser homogéneos para todos los usuarios.

- ✓ Ningún empleado, podrá formatear los discos duros de los computadores.

- ✓ Ningún empleado podrá retirar o implementar partes sin la autorización de la Oficina de sistemas.

- ✓ Cada trabajador o contratista que tenga asignado un equipo de la organización deberá asegurarse de su bloqueo mientras este se encuentre desatendido. El Jefe de Medios tecnológicos hará el respectivo control sobre esta directriz y garantizara que para su desbloqueo cada equipo se encuentre protegido con contraseña.

Otras Políticas

- ✓ La dirección IP asignada a cada equipo debe ser conservada y no se debe cambiar sin la autorización del Jefe de Medios Tecnológicos porque esto ocasionaría conflictos de IP'S y esto alteraría el flujo de la red.

- ✓ No llenar el espacio de disco del equipo con música ni videos, ni información que no sea necesaria para el desarrollo de sus tareas con respecto a la entidad.

- ✓ Todo empleado responsable de equipos informáticos debe dejarlo en modo de hibernación al medio día y apagado en la noche lo anterior para ahorrar recursos energéticos y contribuir a la conservación de los equipos.

- ✓ Cada trabajador o contratista que tenga asignado un equipo de la organización deberá asegurarse de su bloqueo mientras este se encuentre desatendido. El Jefe de Medios tecnológicos hará el respectivo control sobre esta directriz y garantizara que para su desbloqueo cada equipo se encuentre protegido con contraseña.

Políticas de Seguridad en Servidor

Se implementara un servidor bien sea físico o en la nube con las siguientes características en su software de desarrollo:

- ✓ Debe existir un reporte de trazabilidad de los usuarios que ingresan, modifican y extraen información de los servidores.
- ✓ Cada usuario deberá tener una carpeta debidamente organizada para que la información a resguardar sea de fácil acceso y ubicación.
- ✓ El Jefe de medios tecnológico estará encargado de asignar cada una de las carpetas y asignar a cada usuario su clave de acceso y asignara los permisos necesarios para que otros usuarios tengan acceso a información de diferentes usuarios

"El correcto manejo de los equipos de sistemas de la empresa es responsabilidad directa de sus empleados".

PROCEDIMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En este apartado se presenta algunas recomendaciones de procedimientos de seguridad de la información de Seguridad Imperio Ltda. Se tomaron en cuenta algunos numerales de control de seguridad de la información definidos en la norma ISO/IEC 27001, para definir los procedimientos de seguridad necesarios.

SEGURIDAD DEL RECURSO HUMANO:

Procedimiento de ingreso y desvinculación del personal:

Desde el ingreso del trabajador y en su proceso de inducción se orienta acerca del cumplimiento de todas las políticas vinculadas al Sistema Integrado de Gestión incluida la presente política. Esta actividad se refuerza periódicamente a través de los procesos de re-inducción.

Desde el ingreso de trabajador se realiza un riguroso proceso de verificación de antecedente como medida de control y la confidencialidad de los datos se establece por la via del contrato de trabajo.

De igual forma al momento de desvinculación y previa notificación del proceso de Recursos Humanos se procede al bloqueo inmediato de claves, usuarios, contraseñas y demás llaves de acceso.

La entrega de equipos es requisito indispensable en el proceso de paz y salvo.

Procedimiento de capacitación y sensibilización del personal:

Seguridad Imperio Ltda., incorpora en su programa de capacitación temas en relación la seguridad de las tecnologías de la información, la protección de datos y la prevención de actividades ilícitas incluidas la corrupción y el soborno.

GESTION DE ACTIVOS:

En este dominio relacionado con la identificación y clasificación de activos de acuerdo a su criticidad y nivel de confidencialidad se pueden definir los siguientes procedimientos:

Procedimiento de identificación y clasificación de activos:

Los activos en Tecnologías de la Información se identifican mediante la Matriz de Control de Tecnologías de la Información OP-FO-031. Esta matriz especifica como son clasificados tanto equipos como usuarios de acuerdo a su nivel de confidencialidad o criticidad.

Los equipos obsoletos o que cumplan su ciclo de vida útil serán dispuestos a través de gestores de residuos debidamente autorizados.

CONTROL DE ACCESO:

En este dominio relacionado con el acceso a la información y a las instalaciones de procesamiento de la información, se pueden generar los siguientes procedimientos:

Procedimiento para ingreso seguro a los sistemas de información:

Seguridad Imperio Ltda., emplea métodos preventivos contra ataques validando los datos completos para ingreso a los sistemas. A todos los colaboradores administrativos se les debe asignar usuarios y contraseñas de acuerdo a su rol.

Los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también incluye al usuario administrador del sistema.

Para el acceso físico a las instalaciones y prevenir intrusiones o accesos no autorizados a la sede se cuenta con el Procedimiento de Control de Acceso y Seguridad Física OP-PC-002

Procedimiento de gestión de usuarios y contraseñas:

Cada persona que acceda a su equipo de cómputo y al sistema debe tener una sola cuenta de usuario. Esto permite realizar seguimiento y control y evita que interfieran las configuraciones de distintos usuarios.

El Jefe de Medios Tecnológicos es el único usuario administrador de cada equipo de cómputo y del sistema. En caso de ausencia, la Gerencia General deberá tener acceso a la contraseña de usuario administrador y designar a quien considere competente para atender algún requerimiento de mantenimiento. Nota: estas deben ser cambiadas mínimo cada 6 meses o al cambio del personal para proteger la información.

SEGURIDAD FÍSICA Y DEL ENTORNO:

Procedimiento de control de acceso físico:

Para el acceso físico a las instalaciones y prevenir intrusiones o accesos no autorizados a la sede se cuenta con el Procedimiento de Control de Acceso y Seguridad Física OP-PC-002

Procedimiento de protección de activos

Todos los equipos se disponen con las medidas necesarias para asegurar su funcionamiento y preservación libres de humedad, fuentes de calor o de otros factores que puedan afectar la integridad del equipo y de la información que contienen.

Procedimiento de retiro de activos:

Todo equipo que sea retirado de las instalaciones podrá ser retirado con autorización del Jefe de Seguridad o de la Gerencia General cuando aplique. Para ello deberá enviar correo electrónico informando su autorización a recepción.

Procedimiento de mantenimiento de equipos:

Seguridad Imperio Ltda., cuenta con un programa de mantenimiento de equipo, procedimiento vinculado al proceso de Compras y Almacén.

SEGURIDAD DE LAS COMUNICACIONES:

Procedimiento de transferencia de información:

La empresa en cumplimiento a lo dispuesto en la ley y en consideración de sus vínculos permanentes u ocasionales de carácter comercial, podrá efectuar transferencia y transmisión de datos personales e información de los titulares.

Para la transferencia de datos personales de los titulares, Seguridad Imperio Ltda., tomará las medidas necesarias para que los terceros conozcan y se comprometan a observar las políticas aplicables, bajo el entendido que la información personal que reciban, únicamente podrán ser utilizada para asuntos directamente relacionados con Seguridad Imperio Ltda., y solamente mientras ésta dure y no podrá ser usada o destinada para propósito o fin diferente.

RELACIONES CON LOS PROVEEDORES:

Procedimiento para el tratamiento de la seguridad en los acuerdos con los proveedores:

Seguridad Imperio Ltda., documenta acuerdos de seguridad con estos asociados de negocio que incluyen compromisos de confidencialidad de la información y de la imagen de la empresa.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN:

Procedimiento adquisición, desarrollo y mantenimiento de software:

Fieles al compromiso con la prevención de actividades ilícitas tales como el contrabando, el lavado de activos, la financiación del terrorismo la corrupción y el soborno Seguridad Imperio Ltda., solo realizara la adquisición de equipo con proveedores legalmente constituidos que permitan el acceso a información verificable de la compra del equipo.

Los contratistas de mantenimiento de hardware y software suscribirán acuerdos de seguridad y confidencialidad de acuerdo a lo permitido por la ley.

Procedimiento de control software:

Los usuarios no pueden instalar, suprimir o modificar el software originalmente entregado en su computador. Es competencia del Jefe de Medios Tecnológicos la instalación de software.

El inventario de software y plataformas se encuentra en la Matriz de Control de Tecnologías de la información OP-FO-031.

ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO:

Procedimiento de gestión de la continuidad de negocio:

El Jefe de Medios Tecnológicos genera copias de respaldo de acuerdo a lo especificado en la matriz de control de TI y considerando la criticidad de la información y del perfil del usuario. Una copia se mantendrá fuera de las instalaciones.

Aprobado y publicado en la ciudad de Bogotá a los 26 días del mes de Mayo de 2023.

TIBITZAITH OLARTE CASTILLO
Gerente General