SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD

POLÍTICA

Dirección Transformación Digital

Autorizó:

Revisó:

Elaboró:

I. OBJETIVO

Salvaguardar la información de la compañía, evitar la fuga de datos, proteger la confidencialidad, integridad y privacidad de los sistemas, datos e información de Grupo Expansión.

II. ALCANCE

La presente política aplica a todos los colaboradores de Grupo Expansión así como al personal temporal, consultores, contratistas y/o terceros autorizados que accedan a la red, sistemas, aplicaciones, datos e información de Grupo Expansión.

III. DEFINICIONES

- Una interpretación amplia del término "Redes, sistemas, datos e información de la Compañía" deberá incluir de manera enunciativa, pero no limitativa lo siguiente:
  - Todas las computadoras desktop y laptops.
  - Dispositivos portátiles e inalámbricos, como son tabletas y smartphones.
  - Medios removibles como unidades de USB, tarjetas de memoria, thumb drives, CDs, y DVDs.
  - Tecnología de Información, sistemas, servidores y aplicaciones.
  - Redes y servicios de la Compañía.
  - Correo electrónico (e-mail), mensajes instantáneos y sistemas de voz mail.
  - Sistemas y servicios por outsourcing.
  - Documentos impresos.
  - Las conversaciones en áreas públicas que pueden ser escuchadas.

- Incidente de seguridad: se refiere a los eventos o acciones que tienen un impacto real o potencial en la seguridad de la información de la Compañía, incluyendo redes, sistemas, aplicaciones, datos e información dentro o en outsourcing por la Compañía.
- Malware es la definición amplia de cualquier programa, archivo o software que es malicioso.
- Trojan horses: archivo o programa que parece ser legítimo y seguro, pero en realidad es malicioso, ocultando en su interior una finalidad diferente a la esperada.
- Spyware: software que de manera consiente o inconsciente se instala y recopila información para ser enviada a terceros.
- Adware: Software que muestra publicidad invasiva y no deseada.
- Virus: tipo de malware perjudicial creado para infectar y replicarse en los dispositivos electrónicos

IV. LINEAMIENTOS/ RESPONSABILIDADES GENERALES

- Esta política esboza los requerimientos de Grupo Expansión (el Grupo) con relación a la protección de redes, sistemas, aplicaciones, datos e información. Estos requerimientos complementan, pero no reemplazan o sustituyen, el *Código de ética y Conducta* del Grupo.
- El Grupo , sus empleados, así como las terceras partes autorizadas, deben cumplir con las leyes, reglamentos y/o cualquier otra disposición vigente aplicable.
- Siempre que los terceros tengan acceso a la red, sistemas, aplicaciones, datos, o información del Grupo, esta política debe ser incluida en el acuerdo preparado por el representante legal del Grupo. Los Gerentes y Supervisores del Grupo deben asegurar que el personal temporal, consultores, contratistas y otros terceros autorizados tengan pleno conocimiento de esta política.
- Los recursos del Grupo pueden ser monitoreados y/o seleccionados para asegurar que las redes, sistemas, aplicaciones, datos e información, no estén comprometidos o usados para cualquier propósito contradictorio a la misión, políticas y procedimientos del Grupo. El uso de redes, sistemas, aplicaciones, datos e información de la compañía, indican tu aceptación a este monitoreo, por lo que aceptas y acuerdas no interferir intencionalmente con, o evitar los controles de seguridad del Grupo.
- Es responsabilidad de todos los colaboradores, personal temporal, consultores, contratistas y otros terceros reportar inmediatamente un incidente sospechoso de seguridad de información al área de Sistemas del Grupo.
- El Grupo, sus colaboradores, así como los terceros autorizadas deben cumplir con las leyes, reglamentos y/o cualquier otra disposición aplicable.
- Los recursos del Grupo pueden ser monitoreados y/o seleccionados para asegurar que las redes, sistemas, aplicaciones, datos e información, no estén comprometidos o usados para cualquier propósito contradictorio a la misión, políticas y procedimientos del Grupo. El uso de redes, sistemas, aplicaciones, datos e información de la compañía, indica tu aceptación a este monitoreo, por lo que aceptas y acuerdas no interferir intencionalmente con, o evitar los controles de seguridad del Grupo.
- Sólo personas autorizadas deben tener acceso a las redes, sistemas, aplicaciones, datos e información del Grupo.
- La red del Grupo debe ser usada exclusivamente para actividades destinadas para los fines del negocio del Grupo.
- El Grupo proporciona sistemas de mensajes como son: e-mail, mensajes instantáneos (IM, Chat) para usos exclusivos destinados para fines del negocio del Grupo.
- Cada usuario es responsable de la protección de las redes, sistemas, aplicaciones, datos e información de la Compañía, desde pérdida, destrucción, robo, así como el regreso o la

eliminación adecuada de la información. Para lo anterior, cada usuario deberá firmar un documento de confidencialidad con el Grupo.

- Software y hardware usados por las redes, sistemas y aplicaciones del Grupo deben cumplir con los estándares y políticas aprobados por el Grupo.
- No divulgar información confidencial, datos y/o materiales que sean propiedad de la Compañía, sin la debida autorización. No utilizar marcas, patentes, dibujos, modelos sin la debida autorización y, en general, ninguna otra propiedad intelectual ni industrial propiedad del Grupo.
- No descargar software desde el internet sin la aprobación del área de Sistemas del Grupo.
- No descargar imágenes, música, video y/o cualquier otra información que no se disponga de licencia o liberada para el uso público.
- No divulgar, publicar, revelar, transmitir y/o de cualquier otra forma disponer de la información confidencial mediante cualquier método posible, para el uso o beneficio de terceros, sin la autorización previa y por escrito del Grupo.
- No utilizar marcas, nombres comerciales, denominaciones y/o razones sociales sin la autorización de su titular.
- La información relacionada con los clientes del Grupo y empleados debe ser salvaguardada para prevenir una divulgación no autorizada o inadvertida.
- Los controles de la seguridad de información deben ser considerados cuando las redes, sistemas, aplicaciones, datos e información son accesados o manejados por terceros .

V. POLÍTICAS

5.1. REPORTES DE INCIDENTES DE SEGURIDAD DE INFORMACIÓN:

5.1.1. Un incidente puede involucrar:

A. Actividad no usual o sospechosa de computadora.

B. Códigos maliciosos, Malware, como son Virus, Trojan horses, Spyware y Adware.

C. Ataques o el uso indebido de los sistemas informáticos.

D. Sistema de acceso no autorizado.

E. Archivos faltantes o alterados.

F. Pérdida o robo de sistemas informáticos u otros dispositivos que contengan información de la Compañía.

G. Pérdida, robo o falta de Información de la Compañía.

H. Comunicación telefónica o electrónica no solicitada o sospechosa que sea confidencial u otra información sensitiva como son passwords u otro dato técnico.

I. Actividad potencial ilegal involucrando sistemas de información.

J. Terceros (ejemplo, negocios, proveedores o medio) de reportar un incidente de seguridad o amenaza potencial para los sistemas de outsourcing por la Compañía.

5.1.1.1. Cómo reportar un incidente:

El colaborador, personal temporal, consultores, contratistas y otros terceros que sospechen de un incidente deben seguir las siguientes reglas:

- Reportar a Sistemas en el siguiente link https://sistemas.grupoexpansion.com
- No continuar con el uso de cualquier sistema que tenga sospecha que haya sido involucrado en un incidente.
- Permitir el acceso al sistema únicamente a la persona (s)que sea (n) aprobada (s) por el comité de Seguridad de la Información.
- Mantener encendida la computadora ya que de lo contrario puede borrar o corromper información importante que puede ser usada para propósitos forenses.
- Desconectar de la red o internet.

5.1.2. DETECCIÓN Y PREVENCIÓN DE VIRUS/MALWARE

5.1.2.1. Código malicioso

- Si sospechas que tienes un software malicioso en tu sistema, repórtalo a sistemas inmediatamente a través de http://sistemas.grupoexpansion.com
- No abras correos inesperados con archivos adjuntos, no hagas clic en ligas en dichos correos o mensajes instantáneos, ni responder al spam.
- No desactives o eludas intencionalmente la seguridad del software o controles del Grupo.
- Nunca introduzcas intencionalmente un software malicioso en las redes y sistemas del Grupo.

Nota: Los sistemas del Grupo están equipados con un software de seguridad para detectar y proteger contra software maliciosos, incluyendo virus, gusanos, spyware o adware.

Este software puede incluir detección de anti-virus, firewall personal, sistemas de detección de intrusión o encriptación.

5.1.3. ACCESO NO AUTORIZADO

- Desconecta o bloquea todos los sistemas o programas cuando no los uses.
- No desactives una función de bloqueo de funciones (ejemplo protector de pantalla, solicitar contraseña y/o cualquier otra que pudiera tener tu equipo).
- Cuando uses una computadora compartida (ejemplo: en el hotel o biblioteca), no abras archivos confidenciales y siempre desconéctate cuando termines. Cerrando sesión, utiliza el modo incógnito de los navegadores de internet.
- Sigue los procedimientos aprobados para la requisición de acceso a las redes, sistemas, aplicaciones, datos e información del Grupo.
- Notifica a Sistemas cuando el acceso ya no es necesario o los requerimientos de acceso han cambiado.
- Los Gerentes y Supervisores del Grupo deben revisar los requerimientos de acceso de usuarios cuando hay algún movimiento de personal o cambio en el estatus de un colaborador o de otro individuo incluyendo terceras partes autorizadas, accesando a las redes, sistemas, aplicaciones, datos e información del Grupo. Esto incluye revisión de sistemas que pueden estar radicados por terceras personas.
- Nunca intentes obtener un acceso no autorizado a cualquier red, sistemas, aplicaciones, datos y/o información.

5.1.4. CONTRASEÑAS

5.1.4.1. Uso correcto de contraseñas:

- Elige contraseñas que sean al menos de 8 caracteres de longitud, utilizando una combinación de letras y al menos dos números, si el sistema o aplicación te lo permite usa frases largas ejemplo “MiautoRojoesmuyVeloz”.
- Utiliza segundo factor de acceso como código SMS, SecurID/Token en todo sistema o aplicación que te lo permitan, de lo contrario cambia tu contraseña al menos cada 90 días o cada vez que pudo estar comprometida su confidencialidad.
- Las contraseñas no deben ser almacenados donde puedan ser accedidas por otros.
- No compartas la información de tus contraseñas o SecurID-token. Si necesitas proveer tu contraseña al personal de Sistemas o de Soporte Técnico por propósitos de solución de problemas, asegúrate de cambiar tu contraseña después de que el incidente haya sido resuelto.
- En caso de pérdida de tu contraseña repórtalo a Sistemas inmediatamente.
- Reporta cualquier uso no autorizado de tu cuenta o contraseña de sistemas o aplicaciones del Grupo a Sistemas inmediatamente.

5.1.4.2. Grupos o cuentas compartidas

- Las cuentas compartidas o de grupo deben ser evitadas, pero si son absolutamente necesarias como cuentas deben cambiar sus contraseñas cuando un miembro del grupo no lo requiera más o deje la empresa.
- Deberá definirse un responsable de la cuenta/contraseña compartida.

5.1.5. ACCESO A INTERNET Y REDES

5.1.5.1. Instalación de conexiones de Red

- No instale o use conexiones de red no aprobadas, como son módems, DSL, o conexiones inalámbricas no oficiales.
- No conecte sistemas o dispositivos no aprobados, como son equipo personal a las redes del Grupo.
- No lleves a cabo monitoreo de la red, escaneo de vulnerabilidades, o la ilegalidad de contraseña a ninguna red, sistemas, aplicación, base de datos o a cualquier dispositivo a menos que sea autorizado por el Grupo.
- No uses aplicaciones de archivos compartidos peer-to-peer como son KaZaA, Morpheus, BitTorrent, DirectConnect u otros.
- No uses servicios no aprobados que permitan el acceso remoto a los recursos del Grupo como son VNC, AnyDesk, TeamViewer.

5.1.6. USO DEL SISTEMA DE MENSAJES DE LA COMPAÑÍA

- No abras adjuntos inesperados o respondas al e-mail de spam (no solicitado).
- No envíes información confidencial sin autorización.
- No re-envíes o distribuyas cadenas de e-mails. El e-mail frecuentemente es usado para enviar virus u otro contenido no apropiado que puede impactar la operación normal de tu computadora.
- No uses los sistemas de mensajes para enviar mensajes que puedan interpretarse como acosadores u ofensivos.
- A menos que sea autorizado, no envíes mensajes desde la cuenta de alguien más, o intentes hacer que un mensaje aparezca como que otro individuo lo esté enviando.
- No configures las cuentas de e-mail del Grupo para que re-envíe automáticamente los e-mails del Grupo a terceras partes o a cuentas personales de e-mail.
- Cuando contestes a los e-mails o uses una lista de distribución, verifica que el receptor para asegurarte que estás enviando la información a las personas apropiadas.

5.1.7. EQUIPO DE SEGURIDAD

- No dejes laptops sin supervisión, dispositivos portátiles y medios removibles (ejemplo, CDs, DVDs o dispositivos USB) en un escritorio o en un área pública de mucho tráfico. Almacena los dispositivos que pueden ser robados fácilmente en una oficina o cajón con llave.
- Destruye los medios extraíbles antes de su eliminación. Contacta a Sistemas para más información.
- Reporta el robo de cualquier equipo del Grupo inmediatamente a Sistemas.
- Cuando un empleado o tercero deja el Grupo o cambia de trabajo o asignación, el jefe inmediato es responsable de asegurarse que el equipo y los dispositivos de acceso, como son credenciales de acceso a aplicaciones, acceso remoto VPN, correo electrónico, etc. sean correctamente recabadas por el área de Recursos Humanos o Sistemas.

5.1.8. ESTÁNDARES DE SOFTWARE Y HARDWARE

- Usa sólo software y hardware aprobado, adquirido o asignado a través de Sistemas, para acceder a las redes, sistemas, aplicaciones, datos e información interna de la Compañía.
- No descargues o instales software desde el Internet.
- Contacta a Sistemas para proyectos que involucren sistemas nuevos o actualizaciones, incluyendo aquellos que sean de outsourcing.

5.1.9. PROPIEDAD INTELECTUAL

- No divulgues información no pública del Grupo (ejemplo: Contenido editorial, memos, e-mail internos, datos de clientes o empleados, estados financieros y/o información financiera no publicada, datos técnicos o cualquier información delicada o confidencial a la que puedas tener acceso con motivo del desarrollo de tus funciones dentro del Grupo) a terceros sin la previa autorización escrita por parte del Grupo.
- Ten cuidado cuando discutes o trabajas sobre algo que sea información no publicada del Grupo en lugares públicos como son: elevadores, metros, salas de espera, etc.
- La información confidencial debe ser asegurada adecuadamente en archivo de gabinetes con cerradura o almacenamiento aprobado fuera de la oficina. No dejes copia de materiales en áreas públicas, como son: copiadoras, salas de reuniones, etc.
- Depura información confidencial incluyendo información personal y/o financiera relacionada con empleados y clientes, desde copias impresas de materiales (ejemplo: contendores de archivos, faxes, etc.) utilizando trituradoras de acuerdo a los procedimiento de retención definidos.
- Avisar por escrito y oportunamente al Director de Recursos Humanos y al Director de Legal y Cumplimiento cualquier uso indebido o divulgación no autorizada por cualquier colaborador o tercero de la información confidencial del Grupo.

- La divulgación, publicación, revelación, transmisión no autorizada o de cualquier otra forma de la información confidencial del Grupo, puede dar lugar a la violación de la Ley Federal de Derechos de Autor, la Ley de Propiedad Industrial, la Ley Federal de Protección al Consumidor, el Código Penal Federal o cualquier otra regulación aplicable.

5.1.10. INFORMACIÓN DE PRIVACIDAD

Cumplimiento y manejo de la protección de información de los clientes y colaboradores.

- Dar cumplimiento a estándares reglamentarios y contractuales para la protección de la información de los clientes y colaboardores, como son números de tarjetas de crédito, número de seguro social, información de salud e información personalmente identificable. Contacta a la Dirección de Legal y Cumplimiento del Grupo para más información.
- Si el proyecto involucra información confidencial de clientes y empleados internacionales, debes consultarlo con la Dirección Legal y Cumplimiento del Grupo, en relación con cualquier requerimiento de datos trans-fronterizos.
- La recolección y almacenamiento de información de clientes y empleados, debe ser tratada como información confidencial en el mismo grado y de la misma manera en la que éste protege la información confidencial del Grupo.
- No divulgar información de clientes o empleados, excepto con base de "necesito saber" siempre y cuando la información confidencial divulgada sea únicamente aquella que fuese necesaria para la realización de la operación y siempre y cuando dicha divulgación no esté prohibida por ley. En este caso contacta a la Dirección Legal y Cumplimiento del Grupo para acuerdos, estándar contractual y confidencial antes de compartir información sensible o confidencial fuera del Grupo.
- Información de clientes como son: nombres, direcciones, direcciones de e-mail, números telefónicos, números de tarjeta de crédito, información demográfica en lo sucesivo Información Personalmente Identificable (PII) debe ser tratada, almacenada y transferida solo con autorización en los sistemas y aplicaciones designados para dicho fin.
- Información de empleados, incluyendo números de Seguro Social, números de identificación nacional, salud, o información financiera, debe ser tratada, almacenada y transferida solo con autorización en los sistemas y aplicaciones designados para dicho fin.
- Evitar almacenar datos de clientes y/o empleados en laptops o medios removibles (ejemplo: dispositivos USB, thumb drives, CDs, DVDs, etc.) a menos que sea estrictamente necesario, justificado y aprobado por tu jefe inmediato.
- No colectar, procesar, transmitir y/o almacenar información de tarjetas de crédito sin la consulta y aprobación del comité de Seguridad de Información.

5.1.11. ACTIVIDADES DE CONSULTORES, OUTSOURCING Y TERCERAS PARTES.

- Un contrato aprobado por el representante legal del Grupo es requerido para todas las actividades de terceros que incluye el desarrollo de un soporte de redes, sistemas, aplicaciones o procesamiento de datos o información. Ejemplo: Incluye terceras partes que construyen y hospedan sitios web del Grupo, servicios de mercadotecnia e-mail, análisis de sitios web, almacenamiento fuera de la oficina, proveedores de modelos de servicio, etc. Estos sistemas y servicios deben ser revisados por la Dirección de Sistemas y aprobado por el comité de seguridad de información antes de ser lanzados.
- Los sistemas internos que requieran ser accedidos por terceras personas, debe ser solicitado a Sistemas, previa autorización del Director del área y definido del responsable interno antes que su acceso sea otorgado.
- Las conexiones de terceross estarán documentadas y deben ser revisadas anualmente para asegurar que ellos están aún requeridos para el negocio y que sólo usuarios autorizados tienen acceso. Esta revisión es la responsabilidad del patrocinador de negocios.
- El acceso por terceros a las redes, sistemas, aplicaciones, datos e información del Grupo deben ser otorgados para máximo un año, en donde en ese tiempo el patrocinador de negocio debe notificar a Sistemas de la Información por escrito si el acceso aún es requerido.

VI. SANCIONES

El cumplimiento de esta política es de carácter obligatorio, los reportes de violación a la misma serán investigados, y puede resultar en una acción disciplinaria y/o legal, y en el caso de un tercero podrán derivar en la terminación del servicio o rescisión de contrato.

VII. CONTROL DE CAMBIOS.

DESCRIPCION DEL CAMBIO	FECHA	VERSIÓN
Creación del documento	04-Octubre-2023	00