POLÍTICA DE CIBERSEGURIDAD

OBJETIVO

Nuestra Política de Ciberseguridad presenta nuestros lineamientos y disposiciones para preservar la seguridad de nuestra infraestructura tecnológica, datos y sistemas. Cada vez dependemos más de la tecnología para recopilar, almacenar y administrar información y de servicios de terceros, lo que nos vuelve más vulnerables a sufrir graves violaciones de seguridad. Los errores humanos, los ataques cibernéticos y vulnerabilidades de los sistemas podrían causar un gran daño financiero y poner en peligro la reputación de nuestra Compañía. Por esta razón, hemos implementado una serie de medidas de seguridad. De igual forma hemos preparado instrucciones que pueden ayudar a mitigar los riesgos de seguridad. Hemos descrito ambas disposiciones en esta Política.

ALCANCE

Esta Política es aplicable a todos nuestros colaboradores, colaboradoras, contratistas y cualquier persona que tenga acceso permanente o temporal a todos nuestros sistemas, datos y/o hardware.

1. DEFINICIONES

Los términos a continuación tienen los siguientes significados (todos los términos que se utilicen en forma singular en este documento tendrán el mismo significado cuando se utilicen en forma plural).

CONCEPTO	DEFINICIÓN
CIBERSEGURIDAD	Es el conjunto de prácticas, conocimientos, personas, marcos de referencia, metodologías, herramientas y tecnologías comprendidas dentro de varias estrategias que refieren a la posición defensiva que mantiene la organización ante un determinado ataque, evento o brechas de seguridad, lo anterior incluye un programa de prevención, detección y respuesta.
CONFIDENCIALIDAD	La confidencialidad se refiere a la propiedad de la información que implica que solo las personas autorizadas tienen acceso y conocimiento de dicha información. En el contexto de la seguridad de la información, la confidencialidad implica que los datos sensibles o privados están protegidos contra el acceso o divulgación no autorizados.
SOFTWARE	Programa o conjunto de instrucciones computacionales, así como sus datos asociados, procedimientos y pautas que permiten realizar distintas tareas en un sistema informático.
ANTIVIRUS	Tipo de software que se utiliza para evitar, buscar, detectar y eliminar virus de una computadora.
CLICKBAIT	Técnica de escritura que tiene como objetivo, conseguir visitas a alguna página web con el fin de aumentar ingresos publicitarios.
PHISHING	Técnica para engañar a los usuarios explotando su falta de precaución y exceso de confianza para obtener información personal como contraseñas, tarjetas de crédito, cuentas bancarias etc. mediante una copia de la página web legítima o a través de comunicaciones por email o mensajería en las que se suplanta la identidad de la empresa original.
MALWARE	Cualquier programa o código malicioso que tiene la intención de explotar vulnerabilidades en los sistemas con el propósito de causar daños y sustraer información confidencial.

2. INFORMACIÓN CONFIDENCIAL

- Los datos confidenciales son secretos y valiosos. Algunos ejemplos comunes son:
  - Información financiera no publicada.
  - Datos de clientes, socios, proveedores y otros grupos de interés.
  - Patentes, anuncios de televisión, dossiers, contratos, fórmulas o nuevas tecnologías.
  - Listas de clientes (existentes y prospectivos).
  - Bases de datos corporativas.

Todos los colaboradores, colaboradoras, socios, proveedores y contratistas están obligados a proteger estos datos y cualquier otro derivado de los datos originales. En esta Política, presentamos instrucciones para nuestros colaboradores y colaboradoras sobre cómo evitar violaciones de seguridad. Toda información o elemento digital considerado por Genomma Lab Internacional como confidencial debe estar protegido.

3. PROTECCIÓN DE DISPOSITIVOS PERSONALES Y DE LA COMPAÑÍA

Cuando los colaboradores y colaboradoras usan sus dispositivos digitales para acceder a los correos electrónicos o cuentas de la Compañía, introducen un riesgo de seguridad para nuestros datos. Aconsejamos a nuestros colaboradores y colaboradoras que mantengan seguros tanto sus computadoras personales, tabletas y teléfonos celulares como los de la Compañía. Las recomendaciones para asegurar los dispositivos son las siguientes:

- Mantener todos los dispositivos protegidos con contraseña cambiándola regularmente.
- Verificar que las computadoras asignadas cuenten con el antivirus corporativo.
- Asegurarse de no dejar los dispositivos expuestos, esto es, sin los bloqueos necesarios que permitan a cualquier otra persona el uso del dispositivo personal.
- Verificar la disponibilidad de las actualizaciones de las aplicaciones, navegadores y sistemas operativos mensualmente o tan pronto como haya actualizaciones disponibles que deban ser instaladas.
- Reiniciar diariamente los equipos de cómputo para asegurar que las actualizaciones se instalan adecuadamente.
- Iniciar sesión en las cuentas y sistemas de la Compañía sólo a través de redes seguras y privadas.
- Reportar de manera inmediata a "Mesa de Ayuda" (mesadeayuda@genommalab.com) cualquier incidente de seguridad, incluidos la pérdida temporal o definitiva de los equipos, así como el robo.

Se debe evitar acceder a sistemas internos y cuentas desde los dispositivos de otras personas o prestar sus propios dispositivos a otros/as.
En caso de tener que acceder a infraestructura tecnológica o sistemas de la Compañía desde otros dispositivos, se deberá asegurar el cierre de todas las sesiones y la eliminación de cualquier información.
Si no se cuenta con la característica de seguridad de doble factor de autentificación para el correo electrónico, se deberá solicitar a "Mesa de Ayuda" (mesadeayuda@genommalab.com).

Cuando nuevos colaboradores y colaboradoras reciban equipos o dispositivos electrónicos emitidos por la Compañía, recibirán instrucciones acerca de:

- Uso apropiado de contraseñas y cumplimiento de las políticas sobre contraseñas.
- Uso de software antivirus/antimalware.
- Recomendaciones para el uso adecuado de los dispositivos.

Deben seguir las instrucciones para proteger sus dispositivos y consultar a nuestros ingenieros de "Mesa de Ayuda" (mesadeayuda@genommalab.com) si tienen alguna inquietud o pregunta.

4. SEGURIDAD PARA LOS CORREOS ELECTRÓNICOS

Los correos electrónicos a menudo alojan estafas y software malicioso (por ejemplo, virus). Para evitar la infección por virus o el robo de datos:

- Evitar abrir archivos adjuntos y hacer clic en los enlaces cuando el contenido no se explica adecuadamente (por ejemplo, "mire este video, es increíble").
- Sospechar de los títulos de clickbait (por ejemplo, ofreciendo premios o consejos).
- Verificar el correo electrónico y los nombres de las personas de quienes se reciben mensajes para asegurarse de que provengan de cuentas legítimas.
- Buscar inconsistencias (por ejemplo, errores gramaticales, mayúsculas o un número excesivo de signos de exclamación).

Si un colaborador o colaboradora no confía en la procedencia de algún correo electrónico recibido y tiene la sospecha de que no es seguro, puede consultar a nuestra "Mesa de Ayuda" (mesadeayuda@genommalab.com). Si existe la sospecha de haber sido víctima de algún ataque que comprometa la seguridad de la información se deberá reenviar el correo a la cuenta: 911@genommalab.com

Se enviarán notificaciones a la Compañía en los casos en donde exista algún riesgo de Ciberseguridad que deba ser dado a conocer y ante el cual haya que tomar medidas de prevención extraordinarias.

5. CORRECTA GESTIÓN DE CONTRASEÑAS

Las fugas de contraseñas son peligrosas ya que pueden comprometer toda nuestra infraestructura. Las contraseñas no sólo deben ser seguras para que no sean fácilmente hackeadas, sino que también deben permanecer en secreto.

Las cuentas de usuario y las contraseñas NUNCA deben compartirse. Genomma Lab Internacional considerará estos, como delitos graves, que pueden resultar en la terminación de la relación laboral y acciones legales contra los culpables. Por esta razón, aconsejamos a nuestros colaboradores y colaboradoras:

- **Elegir contraseñas con al menos ocho caracteres**, (incluidas letras mayúsculas y minúsculas, números y símbolos) y evite información que pueda adivinarse fácilmente (por ejemplo, cumpleaños).
- **Recordar las contraseñas en lugar de escribirlas.** Si los colaboradores y colaboradoras necesitan escribir sus contraseñas, están obligados a mantener la confidencialidad del documento en papel o digital y destruirlo cuando terminen su trabajo.
- **Cambiar sus contraseñas de acuerdo a la política de contraseñas de los diferentes recursos tecnológicos: redes, sistemas corporativos (SAP, Dynamics, etc.).** Recordar una gran cantidad de contraseñas puede ser complicado. Los servicios de una herramienta de administración de contraseñas se utilizarán para generar y almacenar contraseñas de manera segura. En caso de utilizar los servicios de una herramienta de administración de contraseñas, los colaboradores y colaboradoras están obligados a crear una contraseña segura para la misma herramienta, siguiendo los consejos mencionados anteriormente.

6. TRANSFERENCIA SEGURA DE DATOS

La transferencia de datos presenta riesgos de seguridad. Para prevenirlos:

- Evita transferir datos confidenciales (por ejemplo, información del cliente o registros de empleados) a otros dispositivos o cuentas a menos que sea absolutamente necesario. Cuando se requiere la transferencia masiva de dichos datos, pedimos a los colaboradores y colaboradoras que soliciten ayuda a nuestra "Mesa de Ayuda" (mesadeayuda@genommalab.com).
- Comparte datos confidenciales a través de la red/sistema de la Compañía y no a través de Wi-Fi público o conexión privada.
- Utilizar para la transferencia de datos, solo los recursos tecnológicos que la compañía pone disponibles para tales fines descartando el uso de servicios públicos en la nube (DropBox, WeTransfer, Google Drive, etc.).
- Asegúrate de que los destinatarios de los datos sean personas u organizaciones debidamente autorizadas y tengan políticas de seguridad adecuadas.
- Informa estafas, violaciones de privacidad e intentos de hackeo.

Nuestro servicio de “Mesa de Ayuda” (mesadeayuda@genommalab.com) requiere conocer sobre estafas, infracciones y malware con el fin de proteger nuestra infraestructura de la mejor manera. Por este motivo, aconsejamos a nuestros colaboradores y colaboradoras que informen a nuestros especialistas sobre ataques percibidos, correos electrónicos sospechosos o intentos de suplantación de identidad lo antes posible.

Nuestros Ingenieros de TI deben investigar con prontitud, resolver el problema y enviar una alerta a toda la empresa cuando sea necesario. Nuestros Especialistas en Seguridad son responsables de asesorar a los y las colaboradoras sobre cómo detectar correos electrónicos fraudulentos. Alentamos a nuestros colaboradores y colaboradoras a ponerse en contacto con ellos por cualquier pregunta o inquietud.

7. MEDIDAS ADICIONALES

Para reducir la probabilidad de violaciones de seguridad se deberá considerar lo siguiente:

- El staff ejecutivo de la Compañía y líderes deberán ser responsables y colaborar en la divulgación y adopción de la Política de Ciberseguridad.
- Todos los colaboradores y colaboradoras deberán consultar los recursos (cursos, manuales, documentación) provistos por el área de TI para capacitarse.
- Apagar sus pantallas y bloquear los dispositivos cuando no sean utilizados. Brindar la seriedad y el tiempo necesarios cuando los y las colaboradoras sean requeridos por Mesa de Ayuda y/o personal de TI para

atender los incidentes, brechas o vulnerabilidades.

- Informar sobre los equipos robados o dañados lo antes posible a los departamentos de Recursos Humanos, TI y Legal.
- Cambiar todas las contraseñas de la cuenta inmediatamente cuando se robe un dispositivo.
- Informar sobre alguna amenaza percibida o una posible debilidad de seguridad en los sistemas de la Compañía.
- Abstenerse de descargar o instalar software no autorizado en el equipo de la Compañía.
- Evitar acceder a sitios web sospechosos, sitios de juegos y de apuestas, de contenidos para adultos, etc.
- Evitar el uso de aplicaciones públicas de mensajería, redes sociales o correos personales para compartir información de la Compañía. Por ejemplo. al utilizar WhatsApp, aunque los datos estén cifrados, los mismos se encuentran a disposición de otras compañías (Facebook/Meta).

8. RESPONSABILIDADES DEL DEPARTAMENTO DE TI

- Instalar firewalls, software antimalware y acceder a sistemas de autenticación.
- Gestionar la capacitación en seguridad para todos los colaboradores/as.
- Informar a los colaboradores regularmente sobre nuevos correos electrónicos o virus de estafa y formas de combatirlos.
- Investigar las brechas de seguridad a fondo.
- Seguir las disposiciones de esta Política como lo hacen otros colaboradores/as.
- Generar informes diarios con estadísticas sobre el correo electrónico entrante de dominios externos con actividad sospechosa.
- Ser informado por el departamento de Recursos Humanos sobre la contratación y despidos de colaboradores/as para tomar las medidas apropiadas sobre la disponibilidad de cuentas y equipos electrónicos, etc. Nuestra Compañía tendrá todos los escudos físicos y digitales para proteger la información.

9. TRABAJO EN CASA Y TRABAJO REMOTO

Los colaboradores y colaboradoras remotos deberán seguir las instrucciones de esta Política sin excepción alguna. Dado que accederán a las cuentas y los sistemas de la Compañía desde la distancia, también están obligados a seguir todos los cifrados de datos, estándares y configuraciones de protección, y garantizar que su red privada sea segura. Los colaboradores y colaboradoras deberán estar conectados a través de VPN y/o mediante cualquier otro método de cifrado, también mediante políticas de contraseñas implementadas por el Departamento de TI. Los alentamos a buscar asesoramiento de nuestros Especialistas en Seguridad y Administradores de TI.

10. ACCIONES DISCIPLINARIAS

Esperamos que todos nuestros colaboradores sigan esta Política. Aquellos que causen violaciones de seguridad pueden enfrentar medidas disciplinarias:

- Violación de seguridad por primera vez, no intencional, a pequeña escala: Se puede emitir una advertencia verbal y capacitar al empleado en temas de seguridad.
- Infracciones intencionales, repetidas o de gran escala (que causan daños financieros u otros daños graves): Invocaremos medidas disciplinarias más severas que pueden llegar a ser la terminación de la relación laboral.
- Examinaremos cada incidente caso por caso. Además, los colaboradores/asque no respeten las instrucciones de seguridad enfrentarán una disciplina progresiva, incluso si su comportamiento no ha resultado en una violación de seguridad.

Todo el equipo Genomma Lab Internacional, desde nuestros clientes y socios hasta nuestros colaboradores, colaboradoras y contratistas, deben sentir que sus datos están seguros. La única forma de ganar su confianza es proteger proactivamente nuestros sistemas y bases de datos. Todos podemos contribuir a esto siendo vigilantes y teniendo en cuenta la ciberseguridad en todo momento.

Marco Sparvieri
CEO
April, 2023