Política de Ciberseguridad

Genomma Lab. Internacional

Propósito

Nuestra **Política de Ciberseguridad** presenta nuestros lineamientos y disposiciones para **preservar la seguridad de nuestra infraestructura de datos y tecnología**.

Cada vez dependemos más de la tecnología para recopilar, almacenar y administrar información, lo que nos vuelve más vulnerables a sufrir graves violaciones de seguridad. Los errores humanos, los ataques cibernéticos y el mal funcionamiento del sistema 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, contratistas y cualquier persona que tenga acceso permanente o temporal a nuestros sistemas y/o *hardware*.**

Política

Información confidencial

Los datos confidenciales son secretos y valiosos. 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 corporativos

Todos los colaboradores, 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 sobre cómo evitar violaciones de seguridad.

Toda **información o elemento digital considerado por Genomma Lab como confidencial debe estar protegido**.

Protegemos los dispositivos personales y de la Compañía

Cuando los colaboradores 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 que mantengan seguros tanto sus computadoras personales, tabletas y teléfonos celulares como los de la Compañía**. Para asegurarse de esto:

- Mantén todos los **dispositivos protegidos con contraseña cambiándola regularmente**.
- Elije y actualiza un **software de antivirus completo**.
- Asegúrate de **no dejar sus dispositivos expuestos o desatendidos**.
- **Instala actualizaciones de seguridad de navegadores** y sistemas operativos **mensualmente** o tan pronto como haya actualizaciones disponibles.
- **Inicia sesión en las cuentas** y sistemas de la empresa **sólo a través de redes seguras y privadas**.

También **aconsejamos** a nuestros colaboradores evitar **acceder a sistemas internos y cuentas desde los dispositivos de otras personas o prestar sus propios dispositivos a otros**.

Cuando nuevos colaboradores reciban equipos o dispositivos electrónicos emitidos por la Compañía, recibirán instrucciones a cerca de:

- Uso apropiado de contraseñas y cumplimiento de las políticas sobre contraseñas.
- Uso de *software antivirus/antimalware*

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

Mantener los correos electrónicos seguros

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

- **Evita abrir archivos adjuntos y hacer clic en los enlaces** cuando el contenido no se explica adecuadamente **(por ejemplo, "mire este video, es increíble")**.
- **Sospecha de los títulos de *clickbait*** (por ejemplo, ofreciendo premios o consejos).
- **Verifica el correo electrónico y los nombres de las personas de quienes recibiste un mensaje** para asegurarse de que sean legítimos.
- **Busca inconsistencias** (por ejemplo, errores gramaticales, mayúsculas o un número excesivo de signos de exclamación).

Si un colaborador no está seguro de que un correo electrónico que ha recibido es seguro, puede consultar a nuestra "Mesa de Ayuda" (mesadeayuda@genommalab.com).

Se compartirá una comunicación periódica con la empresa sobre *anti-pishing* y *malware*, dando consejos e instrucciones de seguridad sobre mensajes sospechosos.

Gestionar contraseñas correctamente

Las fugas de contraseña 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 considerará estos 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:

- **Elije contraseñas con al menos ocho caracteres,** (incluidas letras mayúsculas y minúsculas, números y símbolos) y evite información que pueda adivinarse fácilmente (por ejemplo, cumpleaños).
- **Recuerda contraseñas en lugar de escribirlas**. Si los colaboradores necesitan escribir sus contraseñas, están obligados a mantener la confidencialidad del documento en papel o digital y destruirlo cuando terminen su trabajo.
- **Cambia tus contraseñas cada dos meses**. 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. Los colaboradores están obligados a crear una contraseña segura para la herramienta misma herramienta, siguiendo los consejos mencionados anteriormente.

Transferir datos de forma segura

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 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**.
- **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.

Nuestra "Mesa de Ayuda" (mesadeayuda@genommalab.com) requiere saber sobre estafas, infracciones y *malware* para que puedan proteger mejor nuestra infraestructura. Por este motivo, aconsejamos a nuestros colaboradores 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 colaboradores sobre cómo detectar correos electrónicos fraudulentos. Alentamos a nuestros colaboradores a comunicarse con ellos con cualquier pregunta o inquietud.

Medidas adicionales

Para reducir la probabilidad de violaciones de seguridad:

- Apaga sus pantallas y bloquea tus dispositivos al dejar tu lugar de trabajo.
- Informa sobre los equipos robados o dañados lo antes posible a los departamentos de Recursos Humanos, TI y Legal.
- Cambia todas las contraseñas de la cuenta inmediatamente cuando se robe un dispositivo.
- Informa sobre alguna amenaza percibida o una posible debilidad de seguridad en los sistemas de la Compañía.
- Abstente de descargar software sospechoso, no autorizado o ilegal en el equipo de la Compañía.
- Evita acceder a sitios web sospechosos.
- Evita acceder a sitios web de juegos de apuestas, uso responsable de internet y redes sociales

Nuestro departamento de TI debe

- Instalar *firewalls, software antimalware* y acceder a sistemas de autenticación.
- Gestionar la capacitación en seguridad para todos los colaboradores.
- 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.
- 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 empleados 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.

Trabajo en casa y trabajo remoto

Los colaboradores remotos también deben seguir las instrucciones de esta Política. 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 deberán estar conectados a través de VPN y/o mediante cualquier otro método de cifrado, también mediante políticas de contraseña implementadas por el Departamento de TI.

Los alentamos a **buscar asesoramiento de nuestros** Especialistas en Seguridad y Administradores de TI.

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 puede llegar a ser la terminación de la relación laboral.
- Examinaremos cada incidente caso por caso. Además, los colaboradores que no respeten las instrucciones de seguridad enfrentarán una disciplina progresiva, incluso si su comportamiento no ha resultado en una violación de seguridad.

Toma la seguridad en serio

Todo el equipo Genomma Lab, desde nuestros clientes y socios hasta nuestros colaboradores 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.

Jorge Luis Brake Valderrama
Director General
Junio, 2020