2019

IntegraCorp & H
Consulting, S.A. de C.V.

POLÍTICA DE SEGURIDAD CIBERNÉTICA

INTEGRACORP & H CONSULTING

PROPÓSITO

La política de seguridad cibernética de nuestra compañía describe nuestras directrices y disposiciones para preservar la seguridad de nuestra infraestructura de datos y tecnología.

Los errores humanos, los ataques de piratas informáticos y el mal funcionamiento del sistema podrían causar un gran daño y poner en peligro la reputación de nuestra empresa.

Por esta razón, hemos implementado una serie de medidas de seguridad. También hemos preparado instrucciones que pueden ayudar a mitigar los riesgos de seguridad.

ALCANCE

Esta política aplica para todos los empleados, contratistas y becarios además de todo aquel que tenga acceso temporal o permanente a nuestros sistemas y hardware.

ELEMENTOS DE LA POLÍTICA

La confidencialidad de los datos es secreta e invaluable. nuestro enfoque está en los siguientes puntos:

- No publicar información sensible de los clientes en sitios o foros relacionados al giro del cliente.
- Datos de clientes, socios comerciales o vendedores.
- Lista de clientes o prospectos.

Todos nuestros empleados están obligados a proteger esta información. En esta política nosotros proporcionamos a nuestros empleados las instrucciones de cómo evitar estos casos.

PROTEGER DISPOSITIVOS PERSONALES Y DE LA COMPAÑÍA

Mantener segura su computadora, tableta y teléfono celular personal o de la empresa hacemos énfasis en los siguientes puntos:

- Mantener todos los dispositivos protegidos con contraseña.
- Instalación o actualización del software corporativo.
- Asegurarse de no dejar sus dispositivos expuestos o sin atención.

- Instalación de actualizaciones de software mensualmente mínimo o cuando lo requiera el SO, navegadores o herramientas usadas en el desarrollo o de trabajo.
- Ingresar a las cuentas de la compañía solo mediante redes privadas seguras.

Evitar el acceso a sistemas internos y cuentas desde los dispositivos de otras personas o que presten sus propios dispositivos a personas ajenas a la empresa.

Cuando personal nuevo es contratado proporcionar lo siguiente:

- Computadora personal.
- Instalación de software antivirus y malware corporativo.
- Credenciales para acceso a las instalaciones.
- Credenciales para el acceso a software corporativo.

CORREO ELECTRÓNICO

Los correos electrónicos a menudo contienen fraudes o software malicioso. Para evitar la infección de virus o el robo de datos, seguir las siguientes instrucciones:

- Evite abrir archivos adjuntos y hacer clic en los enlaces cuando el contenido no esté adecuadamente explicado (por mira este video etc.).
- Sospeche de los títulos clickbait (por ejemplo, ofreciendo premios, consejos).
- Verifique el correo electrónico y los nombres de las personas de las que recibieron un mensaje para asegurarse de que sean legítimos.

ADMINSTRACIÓN DE CONTRASEÑAS

Las pérdidas de contraseña son peligrosas ya que pueden comprometer toda nuestra infraestructura. No solo las contraseñas deben ser seguras para que no sean pirateadas fácilmente, sino que también deben permanecer en secreto. Por esta razón, aconsejamos a nuestros empleados que:

- Elija contraseñas con al menos ocho caracteres (incluidas letras mayúsculas y minúsculas, números y símbolos) y evite la información que pueda adivinarse fácilmente (por ejemplo, cumpleaños).
- Recuerde las contraseñas en lugar de escribirlas. Si los empleados necesitan escribir sus contraseñas, están obligados a mantener la confidencialidad del documento en papel o digital y destruirlo cuando finalice su trabajo.

- Cambie credenciales solo cuando sea absolutamente necesario. Cuando no es posible intercambiarlos en persona, los empleados deben preferir el teléfono en lugar del correo electrónico, y solo si reconocen personalmente a la persona con la que están hablando.

TRANSFERENCIA DE DATOS

Para la transferencia de datos los empleados deben:

- Evite transferir datos confidenciales (por ejemplo, información del cliente, registros de empleados) a otros dispositivos o cuentas a menos que sea absolutamente necesario.
- Comparta datos confidenciales a través de la red / sistema de la empresa y no a través de Wi-Fi pública.
- Asegúrese de que los destinatarios de los datos sean personas u organizaciones debidamente autorizadas y cuenten con políticas de seguridad adecuadas.

Para reducir la probabilidad de violaciones de seguridad, también instruimos a nuestros empleados a:

- Apague sus pantallas y bloquee sus dispositivos al salir de sus escritorios.
- Reporte el equipo robado o dañado lo más pronto posible al Departamento de Recursos Humanos o TI.
- Cambie todas las contraseñas de cuenta a la vez cuando se roba un dispositivo.
- Reportar una amenaza percibida o una posible debilidad de seguridad en los sistemas de la compañía.
- Abstenerse de descargar software sospechoso, no autorizado o ilegal en el equipo de su empresa.
- Evitar el acceso a sitios web sospechosos

Nuestro Administrador de TI debe:

- Instalar firewalls, software anti malware y sistemas de autenticación de acceso.
- Hacer arreglos para la capacitación de seguridad a todos los empleados.
- Informar regularmente a los empleados acerca de nuevos correos electrónicos o virus de estafa y formas de combatirlos.
- Investigar las violaciones de seguridad a fondo.
- Seguir estas disposiciones de políticas como lo hacen otros empleados.

ACCIONES DISCIPLINARIAS

Esperamos que todos nuestros empleados sigan siempre esta política y quienes causen violaciones de seguridad pueden enfrentar una acción disciplinaria:

- Infracción de seguridad a pequeña escala, no intencional, por primera vez: Podemos emitir una advertencia verbal y capacitar al empleado sobre seguridad.
- Infracciones intencionales, repetidas a gran escala (que causan daños graves o de otro tipo): Invocaremos medidas disciplinarias más severas que pueden incluir el despido. Examinaremos cada incidente caso por caso.