

Contenido

1. Declaración de política  **3**

2. Propósito  **3**

3. Ámbito de aplicación  **4**

4. Elementos clave de la política  **4**

5. Plan y procesos  **4**

6. Clasificación de los sistemas informáticos  **8**

7. Clasificaciones de redes de área local (LAN)  **8**

8. Amenazas a la seguridad  **9**

9. Responsabilidades del usuario  **9**

10. Clasificación de usuarios  **11**

11. Control de acceso  **12**

12. Sanción por violación de la seguridad  **15**

13. Manejo de incidentes de seguridad  **16**

14. Revisión y aprobación  **17**

15. Referencias y documentos relacionados  **17**

1. Declaración de política

La Ley de Protección de Datos de Mauricio de 2017 (la “LPD”) regula el futuro procesamiento de todos los datos personales en Mauricio. Redactada en torno a un conjunto de principios de privacidad reconocidos internacionalmente, la LPD proporciona un marco integral de derechos y deberes diseñados para brindar a las personas un mayor control sobre sus datos personales.

Cuanto más dependamos de la tecnología para recopilar, almacenar y gestionar información, más vulnerables seremos a graves infracciones de seguridad. Los errores humanos, los ataques de piratas informáticos y los fallos del sistema podrían causar grandes daños financieros y poner en peligro la reputación de nuestra empresa.

Nos comprometemos a implementar las medidas adecuadas para proteger todos los datos de los que somos responsables, así como a cumplir con todas las disposiciones de las leyes de protección de datos y ciberseguridad de Mauricio. Por este motivo, hemos implementado una serie de medidas de seguridad y hemos preparado instrucciones que pueden ayudar a mitigar los riesgos de seguridad.

1. Objetivo

La Política de Seguridad Cibernética (la “Política”) cumple varios propósitos. El propósito principal es informar a los usuarios de ***Bruce Investments Limited*** (la “Compañía”, “Nosotros” o “Bruce”), incluidos empleados, contratistas y otros usuarios autorizados, sobre sus requisitos obligatorios para proteger los activos tecnológicos y de información de la Compañía, e identificar muchas de las amenazas a dichos activos.

La Política también describe las responsabilidades y privilegios de los usuarios, así como lo que se considera un uso aceptable y las reglas relativas al acceso a Internet. La Política también informa a los usuarios sobre sus limitaciones y sanciones por la violación de la Política, y los procedimientos a seguir al responder a incidentes que amenacen la seguridad de los sistemas informáticos y la red de la Compañía.

La Política describe las pautas y disposiciones de la Compañía para preservar la seguridad de su infraestructura de datos y tecnología.

1. Alcance

Esta Política se aplica a todos nuestros empleados, contratistas, voluntarios y cualquier persona que tenga acceso permanente o temporal a nuestros sistemas y hardware.

1. Elementos clave de la política

Los siguientes son los elementos clave de esta política:

* Procesos de gobernanza y evaluación de riesgos de la ciberseguridad
* Derechos de acceso y controles
* Prevención de pérdida de datos
* Gestión de proveedores
* Capacitación
* Plan de respuesta a incidentes

1. Plan y procesos

| Medida | Disposiciones clave |
| --- | --- |
| Mantenga todos los dispositivos protegidos con contraseña. | 1. Elija y actualice un software antivirus completo. 2. Asegúrese de que los usuarios no dejen sus dispositivos expuestos o desatendidos. 3. Instale actualizaciones de seguridad de navegadores y sistemas mensualmente o tan pronto como estén disponibles. 4. Inicie sesión en las cuentas y sistemas de la empresa únicamente a través de redes seguras y privadas. 5. También aconsejamos a nuestros empleados que eviten acceder a sistemas y cuentas internas desde los dispositivos de otras personas o prestar sus propios dispositivos a otros. 6. Cuando los nuevos empleados reciban el equipo proporcionado por la empresa, recibirán instrucciones para:  * [Configuración del cifrado de disco] * [Configuración de la herramienta de gestión de contraseñas] * [Instalación de software antivirus/antimalware] * Deben seguir las instrucciones para proteger sus dispositivos y consultar a nuestros [especialistas en seguridad/ingenieros de red] si tienen alguna pregunta. |
| Mantenga los correos electrónicos seguros | Los correos electrónicos suelen contener estafas y software malicioso (por ejemplo, gusanos). Para evitar infecciones de virus o robo de datos, les indicamos a los empleados que:   * Evite abrir archivos adjuntos y hacer clic en enlaces cuando el contenido no esté adecuadamente explicado (por ejemplo, “mira este video, es increíble”). * Desconfíe de los títulos clickbait (por ejemplo, que ofrecen premios o consejos). * Verifique el correo electrónico y los nombres de las personas de quienes recibieron un mensaje para asegurarse de que sean legítimos. * Busque inconsistencias o pistas (por ejemplo, errores gramaticales, letras mayúsculas, número excesivo de signos de exclamación). * Si un empleado no está seguro de que un correo electrónico que recibió sea seguro, puede consultar a nuestro departamento de TI. |
| Gestionar contraseñas adecuadamente | Las filtraciones de contraseñas son peligrosas, ya que pueden comprometer toda nuestra infraestructura. Las contraseñas no solo deben ser seguras para que no se puedan piratear fácilmente, sino que también deben permanecer en secreto. Por este motivo, recomendamos a nuestros empleados que:   1. Elija contraseñas con al menos ocho caracteres (incluyendo letras mayúsculas y minúsculas, números y símbolos) y evite información que pueda adivinarse fácilmente (por ejemplo, cumpleaños). 2. Recordar 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 al finalizar su trabajo. 3. Intercambie credenciales solo cuando sea absolutamente necesario. Cuando no sea posible intercambiarlas 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. 4. Cambie sus contraseñas cada dos meses. 5. Adquirimos los servicios de una herramienta de gestión de contraseñas que genera y almacena contraseñas. Los empleados están obligados a crear una contraseña segura para la propia herramienta, siguiendo los consejos mencionados anteriormente. |
| Transferir datos de forma segura | La transferencia de datos presenta riesgos de seguridad. Los empleados deben:   1. Evite transferir datos confidenciales (por ejemplo, información de clientes, registros de empleados) a otros dispositivos o cuentas a menos que sea absolutamente necesario. Cuando sea necesaria la transferencia masiva de dichos datos, solicitamos a los empleados que soliciten ayuda a nuestros [especialistas en seguridad]. 2. Comparta datos confidenciales a través de la red/sistema de la empresa y no a través de Wi-Fi público o conexión privada. 3. Asegurarse de que los destinatarios de los datos sean personas u organizaciones debidamente autorizadas y cuenten con políticas de seguridad adecuadas. |
| Denuncie estafas, violaciones de privacidad e intentos de piratería | Nuestro departamento de TI necesita estar al tanto de las estafas, las infracciones y el malware para poder proteger mejor nuestra infraestructura. Por este motivo, recomendamos a nuestros empleados que informen a nuestros especialistas lo antes posible sobre los ataques percibidos, los correos electrónicos sospechosos o los intentos de phishing. Nuestros [especialistas en TI/ingenieros de redes] deben investigar de inmediato, resolver el problema y enviar una alerta a toda la empresa cuando sea necesario.  Nuestros especialistas en seguridad son responsables de asesorar a los empleados sobre cómo detectar correos electrónicos fraudulentos. Animamos a nuestros empleados a que se pongan en contacto con ellos si tienen alguna pregunta o inquietud. |
| Medidas adicionales | Para reducir la probabilidad de violaciones de seguridad, también instruimos a nuestros empleados a:   1. Apaguen sus pantallas y bloqueen sus dispositivos cuando abandonen sus escritorios. 2. Reporte el equipo robado o dañado lo antes posible al Departamento de Recursos Humanos/TI. 3. Cambie todas las contraseñas de las cuentas a la vez cuando se robe un dispositivo. 4. Informar sobre una amenaza percibida o una posible debilidad de seguridad en los sistemas de la empresa. 5. Abstenerse de descargar software sospechoso, no autorizado o ilegal en los equipos de su empresa. |
| Evite acceder a sitios web sospechosos. | También esperamos que nuestros empleados cumplan con nuestra política de uso de Internet y redes sociales.  Nuestro departamento de TI debe:   * Instalar firewalls, software anti-malware y sistemas de autenticación de acceso. * Organizar capacitación en seguridad para todos los empleados. * Informe periódicamente a los empleados sobre nuevos correos electrónicos fraudulentos o virus y las formas de combatirlos. * Investigar exhaustivamente las violaciones de seguridad. * Siga las disposiciones de esta política como lo hacen los demás empleados. * Nuestra empresa contará con todos los escudos físicos y digitales para proteger la información.   *Empleados remotos*  *Los empleados remotos también deben seguir las instrucciones de esta política. Dado que accederán a las cuentas y sistemas de nuestra empresa a distancia, están obligados a seguir todos los estándares y configuraciones de encriptación de datos y protección, y garantizar que su red privada sea segura.*  *Los animamos a que busquen asesoramiento en nuestro departamento de TI .* |
| Tome la seguridad en serio | Todos, desde nuestros clientes y socios hasta nuestros empleados y contratistas, deben sentir que sus datos están seguros. La única forma de ganarnos su confianza es proteger de forma proactiva nuestros sistemas y bases de datos. Todos podemos contribuir a ello estando alerta y teniendo en cuenta la ciberseguridad. |

1. Clasificación de los sistemas informáticos

| Nivel de seguridad | Descripción | Ejemplo |
| --- | --- | --- |
| ROJO | Este sistema contiene información confidencial, es decir, que no puede revelarse a personal externo a la empresa. Incluso dentro de la empresa, el acceso a esta información se proporciona en función de la necesidad de conocerla.  El sistema proporciona servicios esenciales para el funcionamiento de la empresa. Una falla en este sistema puede tener consecuencias que pongan en riesgo la vida de la empresa o tener un impacto financiero adverso en su actividad. | Servidor que contiene datos confidenciales y otra información del departamento en bases de datos. Enrutadores de red y cortafuegos que contienen tablas de enrutamiento confidenciales e información de seguridad. |
| VERDE | Este sistema no contiene información confidencial ni realiza servicios críticos, pero proporciona la capacidad de acceder a los sistemas RED a través de la red. | PC del departamento de usuarios utilizadas para acceder al servidor y a las aplicaciones.  Estaciones de trabajo de gestión utilizadas por administradores de sistemas y redes. |
| BLANCO | Este sistema no es accesible desde el exterior. Se encuentra en un segmento de LAN aislado y no puede acceder a los sistemas ROJO o VERDE. No contiene información confidencial ni realiza servicios críticos. | Un sistema de pruebas utilizado por diseñadores y programadores de sistemas para desarrollar nuevos sistemas informáticos. |
| NEGRO | Este sistema es accesible desde el exterior. Está aislado de los sistemas ROJO o VERDE mediante un cortafuegos. Si bien realiza servicios importantes, no contiene información confidencial. | Un servidor web público con información no confidencial. |

1. Clasificaciones de redes de área local (LAN)

Una LAN se clasificará según los sistemas conectados directamente a ella. Por ejemplo, si una LAN contiene solo un sistema RED y todos los usuarios de la red estarán sujetos a las mismas restricciones que los usuarios de los sistemas RED, una LAN asumirá la Clasificación de Seguridad de los sistemas de nivel más alto conectados a ella.

1. Amenazas a la seguridad

A continuación se presenta un resumen de las principales amenazas a la ciberseguridad:

Empleados

Una de las mayores amenazas para la seguridad son los empleados. Pueden dañar sus sistemas ya sea por incompetencia o intencionalmente. También debe implementar medidas de seguridad para compensar esto. Puede mitigarlo haciendo lo siguiente.

* Otorgue únicamente los derechos apropiados a los sistemas. Limite el acceso únicamente al horario comercial.
* No comparta cuentas para acceder a los sistemas. Nunca comparta su información de inicio de sesión con compañeros de trabajo.
* Cuando los empleados son separados o disciplinados, se elimina o limita el acceso a los sistemas.
* Avanzado: mantenga registros detallados del sistema sobre toda la actividad de la computadora.
* Proteger físicamente los activos informáticos, de modo que sólo el personal con la necesidad adecuada pueda acceder a ellos.

Hackers aficionados y vándalos.

Estas personas son el tipo más común de atacantes en Internet y, por lo general, implican delitos de oportunidad. Los piratas informáticos aficionados escanean Internet y buscan agujeros de seguridad conocidos que no hayan sido tapados, incluidos los servidores web y el correo electrónico, que son sus objetivos favoritos . Una vez que encuentran una debilidad, la explotarán para plantar virus o troyanos, o utilizar los recursos del sistema de la empresa para sus propios fines. Si no encuentran una debilidad obvia, es probable que pasen a un objetivo más fácil.

Hackers criminales y saboteadores.

La probabilidad de que se produzca este tipo de ataque es baja, pero no del todo improbable dada la cantidad de información sensible que contienen las bases de datos. La habilidad de estos atacantes es media-alta, ya que es probable que estén entrenados en el uso de las herramientas de hackers más modernas. Los ataques están bien planificados y se basan en cualquier debilidad descubierta que les permita introducirse en la red.

1. Responsabilidades del usuario

Esta sección establece la política de uso de los sistemas informáticos, redes y recursos de información de la oficina. Se aplica a todos los empleados y contratistas que utilizan los sistemas informáticos, redes y recursos de información como socios comerciales y a las personas a las que se les concede acceso a la red para los fines comerciales de la Compañía.

Uso aceptable

Las cuentas de usuario en los sistemas informáticos de la Compañía se deben utilizar únicamente para fines comerciales de la Compañía y no para actividades personales. El uso no autorizado del sistema puede constituir una violación de la ley, constituye un robo y puede ser sancionado por la ley. Por lo tanto, el uso no autorizado del sistema informático y las instalaciones de la Compañía puede constituir motivo de procesamiento civil o penal.

Los usuarios son personalmente responsables de proteger toda la información confidencial utilizada y/o almacenada en sus cuentas. Esto incluye sus credenciales de inicio de sesión y contraseñas. Además, tienen prohibido realizar copias no autorizadas de dicha información confidencial y/o distribuirla a personas no autorizadas fuera de la empresa.

Los usuarios no deberán participar intencionalmente en actividades con la intención de: acosar a otros usuarios; degradar el rendimiento del sistema, desviar recursos del sistema para su propio uso u obtener acceso a sistemas de la empresa para los que no tienen autorización.

Los usuarios no deben conectar dispositivos no autorizados a sus computadoras o estaciones de trabajo, a menos que hayan recibido autorización específica del gerente del empleado y/o del representante de TI de la empresa. Los usuarios no deben descargar software no autorizado de Internet a sus computadoras o estaciones de trabajo.

Los usuarios están obligados a informar a su supervisor inmediato sobre cualquier debilidad en la seguridad informática de la empresa, cualquier incidente de mal uso o violación de esta política.

Uso de Internet

La empresa proporcionará acceso a Internet a los empleados y contratistas que estén conectados a la red interna y que tengan una necesidad comercial de dicho acceso. Los empleados y contratistas deben obtener permiso de su supervisor y presentar una solicitud al administrador de seguridad.

Internet es una herramienta comercial para la Compañía. Se utiliza para fines comerciales, como por ejemplo: comunicarse por correo electrónico con clientes y socios comerciales, obtener información comercial útil y temas comerciales y técnicos relevantes.

El servicio de Internet no puede utilizarse para transmitir, recuperar o almacenar ninguna comunicación de naturaleza discriminatoria o acosadora o que sea despectiva hacia cualquier individuo o grupo, obscena o pornográfica, o difamatoria o amenazante por naturaleza para “cartas en cadena” o cualquier otro propósito que sea ilegal o para beneficio personal.

1. Clasificación de usuarios

Se espera que todos los usuarios conozcan esta Política y deben informar las infracciones al administrador de seguridad. Además, todos los usuarios deben cumplir con la sección Uso aceptable de esta Política. La empresa ha establecido los siguientes grupos de usuarios y ha definido los privilegios y responsabilidades de acceso:

| Categoría de usuario | Privilegios y responsabilidades |
| --- | --- |
| Usuarios del Departamento (Empleados) | Acceso a la aplicación y a las bases de datos según sea necesario para la función laboral. (ROJO y/o VERDE habilitados) |
| Administradores de sistemas | Acceso a sistemas informáticos, enrutadores, concentradores y demás tecnología de infraestructura necesaria para el desempeño del trabajo. Acceso a información confidencial únicamente cuando sea necesario. |
| Administrador de seguridad | Nivel más alto de autorización de seguridad. Acceso permitido a todos los sistemas informáticos, bases de datos, cortafuegos y dispositivos de red según lo requiera el puesto de trabajo. |
| Analista de sistemas/programador | Acceso a aplicaciones y bases de datos según sea necesario para la función laboral específica. No está autorizado a acceder a enrutadores, cortafuegos u otros dispositivos de red. |
| Consultores | Acceso a aplicaciones y bases de datos según sea necesario para funciones laborales específicas. Acceso a enrutadores y cortafuegos solo si es necesario para la función laboral. Conocimiento de políticas de seguridad.  El acceso a la información y a los sistemas de la empresa debe ser aprobado por escrito por el director/CEO de la empresa. |
| Otras agencias y socios comerciales | Se permite el acceso a aplicaciones seleccionadas solo cuando existe un contrato o un acuerdo de acceso entre agencias o lo exigen las leyes aplicables. |
| Público general | El acceso está limitado a las aplicaciones que se ejecutan en servidores web públicos. El público en general no podrá acceder a información confidencial. |

Monitoreo del uso de sistemas informáticos

La Compañía tiene el derecho y la capacidad de monitorear la información electrónica creada y/o comunicada por personas que utilizan los sistemas y redes de computadoras de la compañía, incluidos los mensajes de correo electrónico y el uso de Internet. No es la política ni la intención de la compañía monitorear continuamente todo el uso de las computadoras por parte de los empleados u otros usuarios de los sistemas y redes de computadoras de la compañía. Sin embargo, los usuarios de los sistemas deben saber que la compañía puede monitorear el uso, incluidos, entre otros, los patrones de uso de Internet (por ejemplo, el sitio al que se accede, el tiempo que se pasa en línea, la hora del día en que se accede) y los archivos y mensajes electrónicos de los empleados en la medida necesaria para garantizar que Internet y otras comunicaciones electrónicas se estén utilizando de conformidad con la ley y la política de la compañía.

1. Control de acceso

Un componente fundamental de nuestra Política de Seguridad Cibernética es el control del acceso a los recursos de información críticos que requieren protección contra la divulgación o modificación no autorizadas. El significado fundamental del control de acceso es que se asignan permisos a personas o sistemas que están autorizados a acceder a recursos específicos. Los controles de acceso existen en varias capas del sistema, incluida la red. El control de acceso se implementa mediante el ID de inicio de sesión y la contraseña. A nivel de aplicación y base de datos, se pueden implementar otros métodos de control de acceso para restringir aún más el acceso. Los sistemas de aplicaciones y bases de datos pueden limitar la cantidad de aplicaciones y bases de datos disponibles para los usuarios en función de los requisitos de su trabajo.

Acceso al sistema y a la red de usuarios: identificación normal del usuario

Todos los usuarios deberán tener un ID de inicio de sesión y una contraseña únicos para acceder a los sistemas. La contraseña del usuario debe mantenerse confidencial y NO DEBE compartirse con el personal de administración y supervisión ni con ningún otro empleado. Todos los usuarios deben cumplir con las siguientes reglas con respecto a la creación y el mantenimiento de contraseñas:

* La contraseña no debe encontrarse en ningún diccionario inglés o extranjero. Es decir, no utilice ningún nombre común, sustantivo, verbo, adverbio o adjetivo. Estos pueden descifrarse fácilmente utilizando "herramientas de hackers" estándar.
* Las contraseñas no deben publicarse en las terminales de computadora ni cerca de ellas ni ser fácilmente accesibles en el área de la terminal.
* La contraseña debe cambiarse cada (# de días).
* Las cuentas de usuario se congelarán después de (# de días) intentos de inicio de sesión fallidos.
* Los ID de inicio de sesión y las contraseñas se suspenderán después de (# de días) días sin uso.

Los usuarios no pueden acceder a los archivos de contraseñas de ningún componente de la infraestructura de red. Los archivos de contraseñas de los servidores serán monitoreados para detectar el acceso por parte de usuarios no autorizados. Está prohibido copiar, leer, eliminar o modificar un archivo de contraseñas en cualquier sistema informático.

A los usuarios no se les permitirá iniciar sesión como Administrador del sistema. Los usuarios que necesiten este nivel de acceso a los sistemas de producción deben solicitar una cuenta de acceso especial, como se describe en otra parte de este documento.

Los nombres de inicio de sesión y las contraseñas de los empleados se desactivarán lo antes posible si el empleado es despedido, suspendido, puesto en licencia o abandona el empleo en la oficina de la empresa.

Los supervisores/gerentes deben comunicarse de manera inmediata y directa con el Gerente de TI de la empresa para informar cualquier cambio en el estado del empleado que requiera la terminación o modificación de los privilegios de acceso de inicio de sesión del empleado.

Los empleados que olviden su contraseña deberán llamar al departamento de TI para que se les asigne una nueva contraseña a su cuenta. El empleado deberá identificarse ante el departamento de TI mediante (por ejemplo, su número de empleado).

Los empleados serán responsables de todas las transacciones que se realicen durante las sesiones de inicio de sesión iniciadas mediante el uso de la contraseña y el ID del empleado. Los empleados no podrán iniciar sesión en una computadora y luego permitir que otra persona use la computadora o comparta de alguna otra manera el acceso a los sistemas informáticos.

Acceso de administrador del sistema

Los administradores de sistemas, administradores de red y administradores de seguridad tendrán (tipo de acceso) acceso a sistemas host, enrutadores, concentradores y firewalls según sea necesario para cumplir con las tareas de su trabajo.

Todas las contraseñas de administrador del sistema serán ELIMINADAS inmediatamente después de que cualquier empleado que tenga acceso a dichas contraseñas sea despedido, despedido o abandone el empleo en la empresa.

Acceso especial

Las cuentas de acceso especial se proporcionan a personas que requieren privilegios temporales de administrador del sistema para realizar su trabajo. Estas cuentas son supervisadas por la empresa y requieren el permiso del gerente de TI. El control de las cuentas de acceso especial se realiza ingresando a los usuarios en un área específica y generando informes periódicos para la administración. Los informes mostrarán quién tiene actualmente una cuenta de acceso especial, por qué motivo y cuándo caducará.

Conexión a redes de terceros

Esta Política se establece para garantizar un método seguro de conectividad entre la empresa y todas las empresas de terceros y otras entidades requeridas para intercambiar información electrónicamente con la Empresa.

“Terceros” se refiere a proveedores, consultores y socios comerciales que hacen negocios con la Compañía y otros socios que tienen la necesidad de intercambiar información con la Compañía. Las conexiones de red de terceros deben ser utilizadas únicamente por los empleados del tercero, únicamente para los fines comerciales de la Compañía. La empresa de terceros se asegurará de que solo los usuarios autorizados puedan acceder a la información en la red de la Compañía. El tercero no permitirá que el tráfico de Internet u otro tráfico de red privada fluya hacia la red. Una conexión de red de terceros se define como una de las siguientes opciones de conectividad:

* Una conexión de red finalizará en un (a especificar) y el tercero estará sujeto a las reglas de autenticación estándar de la empresa.
* Esta Política se aplica a todas las solicitudes de conexión de terceros y a cualquier conexión de terceros existente. En los casos en que las conexiones de red de terceros existentes no cumplan con los requisitos descritos en este documento, se rediseñarán según sea necesario.

Todas las solicitudes de conexiones con terceros deben realizarse mediante la presentación de una solicitud por escrito y ser aprobadas por la Compañía.

Conexión de dispositivos a la red

Solo los dispositivos autorizados pueden conectarse a las redes de la empresa. Los dispositivos autorizados incluyen computadoras y estaciones de trabajo propiedad de la empresa que cumplan con las pautas de configuración de la empresa. Otros dispositivos autorizados incluyen dispositivos de infraestructura de red utilizados para la administración y el monitoreo de la red.

Los usuarios no podrán conectarse a la red con equipos ajenos a la empresa que no estén autorizados, sean propiedad de la empresa o no estén controlados por ella. Los usuarios tienen prohibido específicamente conectarse (especificar) a la red de la empresa.

NOTA: Los usuarios no están autorizados a conectar ningún dispositivo que altere las características de topología de la red ni ningún dispositivo de almacenamiento no autorizado, por ejemplo, unidades USB y CD grabables.

Acceso remoto

Sólo las personas autorizadas pueden acceder de forma remota a la red de la empresa. El acceso remoto se proporciona a aquellos empleados, contratistas y socios comerciales de la empresa que tengan una necesidad comercial legítima de intercambiar información, copiar archivos o programas o acceder a aplicaciones informáticas. La conexión autorizada puede ser de una PC remota a la red o de una red remota a la red de la empresa. El único método aceptable para conectarse de forma remota a la red interna es mediante una identificación segura.

Acceso remoto no autorizado

No se permite la conexión de concentradores (por ejemplo) a una PC o estación de trabajo de un usuario que esté conectada a la red LAN de la empresa sin el permiso por escrito de la empresa. Además, los usuarios no pueden instalar software personal diseñado para proporcionar control remoto de la PC o estación de trabajo. Este tipo de acceso remoto elude los métodos de acceso remoto de alta seguridad autorizados y supone una amenaza para la seguridad de toda la red.

1. Sanción por violación de seguridad

La empresa se toma muy en serio el tema de la seguridad.

Quienes utilicen la tecnología y los recursos informáticos de la empresa deben saber que pueden ser objeto de medidas disciplinarias si violan esta política. En caso de violación de esta política, un empleado de la empresa puede estar sujeto a medidas disciplinarias que pueden llegar hasta el despido. La medida disciplinaria específica impuesta se determinará caso por caso, teniendo en cuenta la naturaleza y la gravedad de la violación de esta política, las violaciones previas de la política cometidas por el individuo, las leyes estatales y federales y toda otra información pertinente. La medida disciplinaria que pueda tomarse contra un empleado se administrará de conformidad con las normas o políticas correspondientes y la política de la empresa.

En caso de que la persona acusada no sea un empleado de la empresa, el asunto se presentará a (la persona designada por la empresa). La persona designada por la empresa podrá remitir la información a las autoridades competentes o a los fiscales para que consideren si se deben presentar cargos penales contra el presunto infractor.

1. Manejo de incidentes de seguridad

En esta sección se proporcionan algunas pautas y procedimientos de política para gestionar incidentes de seguridad. El término “incidente de seguridad” se define como cualquier evento irregular o adverso que amenace la seguridad, integridad o disponibilidad de los recursos de información en cualquier parte de la red de la empresa. Algunos ejemplos de incidentes de seguridad son:

* Acceso ilegal al sistema informático de una empresa. Por ejemplo, un hacker accede a un servidor de producción y copia el archivo de contraseñas.
* Daños a un sistema informático o red de una empresa causados por un acceso ilegal. Un ejemplo sería la propagación de un virus o un gusano.
* Ataque de denegación de servicio contra un servidor web de una empresa. Por ejemplo, un hacker inicia una avalancha de paquetes contra un servidor web con el objetivo de provocar el bloqueo del sistema.
* Uso malintencionado de los recursos del sistema para lanzar un ataque contra otro equipo fuera de la red de la empresa. Por ejemplo, el administrador del sistema detecta una conexión a una red desconocida y un proceso extraño que acumula mucho tiempo de servidor.
* Los empleados que consideren que sus terminales o sistemas informáticos han sido objeto de un incidente de seguridad o que se ha accedido a ellos o se han utilizado de forma indebida deben informar de la situación a su representante de la empresa de inmediato. El empleado no debe apagar el ordenador ni eliminar archivos sospechosos. Dejar el ordenador en las condiciones en las que se encontraba cuando se descubrió el incidente de seguridad ayudará a identificar la fuente del problema y a determinar los pasos que se deben seguir para solucionarlo.

1. Revisión y aprobación

Esta Política será revisada y aprobada por la junta cada año.

1. Referencias y documentos relacionados

| Políticas asociadas | * Política de Gestión de Riesgos * Marco de gobernanza corporativa |
| --- | --- |
| Referencias/referencias legales | * Ley de Protección de Datos de 2017 * Ley de Tecnologías de la Información y la Comunicación de 2001 |