POLÍTICA DE SEGURIDAD EN LAS COMUNICACIONES

El objetivo de esta política es garantizar la seguridad de las redes y los servicios de red, asegurando la protección de las infraestructuras de comunicación esenciales para las actividades realizadas en el Centro de Arbitraje Latinoamericano e Investigaciones Jurídicas -CEAR LATINOAMERICANO-.

En este sentido, la organización ha definido las siguientes cláusulas:

1. CONTROLES DE LA RED

1.1. El uso de los recursos de red para el acceso a internet deberá ser utilizado con el propósito expreso de realizar tareas relacionadas a las actividades de la organización.

1.2. Todas las conexiones desde las redes de la organización hacia redes externas deben estar protegidas mediante el firewall FortiGate y el servicio de Cloudflare, con el objetivo de fortalecer la seguridad perimetral.

1.3. La información sobre direcciones lógicas internas, configuraciones y detalles de los sistemas de comunicación y cómputo de la organización es confidencial, al igual que la arquitectura y topología de red.

1.4. Los controles de red deben implementarse conforme a los siguientes lineamientos:

- Las direcciones internas, configuraciones e información sobre el diseño de los sistemas de comunicación y cómputo deben estar restringidas.
- La conexión de equipos de cómputo y dispositivos de comunicación de la organización solo debe ser realizada por personal autorizado.
- La red debe contar con mecanismos de detección de intrusos y medidas de protección contra la intercepción de información.
- Se debe garantizar una segmentación adecuada de la red para reforzar la seguridad.

2. REDES DE TELECOMUNICACIONES

2.1. La organización debe garantizar la protección de la información en las redes internas y la seguridad de la infraestructura que las soporta.

2.2. Está prohibido el acceso a conexiones de redes externas dentro de la organización.

2.3. La organización implementará medidas de seguridad para proteger sus redes ante posibles ataques internos y externos, utilizando los recursos tecnológicos más apropiados en cada momento.

Av. Sánchez Carrión Nº 615
Edif. Vértice 22 Oficina 306 - Jesús María - Lima
51-(1) 397 8586 / 51-(1) 957 540 053
arbitraje@cearlatinoamericano.pe
Web: www.cearlatinoamericano.pe

2.4. La organización podrá filtrar las páginas web a las que pueden acceder los usuarios con el objetivo de garantizar el uso profesional del servicio y evitar los riesgos al visitar sitios peligrosos.

2.5. Las redes de la organización deben ser monitoreadas continuamente para prevenir accesos no autorizados, detectar comportamientos anómalos en el tráfico de red y evitar cualquier violación a las políticas de seguridad de la información.

2.6. El encargado de TI podrá revisar periódicamente los registros (*logs*) de los sistemas para verificar su correcto uso, detectar posibles violaciones o ataques, y asegurar su cumplimiento con las políticas, estándares y procedimientos de seguridad.

2.7. Todo nuevo sistema que se instale en la red debe ser evaluado previamente antes de pasar al entorno de producción, siguiendo el proceso de gestión de cambios definido en la organización.

2.8. El encargado TI debe proporcionar controles de contingencia de red, asegurando su operatividad mediante la implementación del plan de continuidad del negocio y el procedimiento de gestión de incidentes.

3. TRANSFERENCIA DE INFORMACIÓN

3.1. La información intercambiada debe ser entregada al destinatario siguiendo los lineamientos de seguridad establecidos.

3.2. Se prohíbe el envío, descarga o visualización de información con contenido que atente contra la integridad moral, personal y/o institucional.

3.3. Cada colaborador es responsable del contenido de la comunicación e información que envíe o descargue desde su cuenta de acceso.

3.4. Se deben implementar mecanismos de detección y protección contra código malicioso en la información transmitida electrónicamente.

3.5. Se debe contar con mecanismos para proteger la información transmitida de intercepción, copiado, modificación, cambio de ruta y destrucción.

3.6. La transferencia de archivos debe realizarse únicamente a través de canales aprobados y seguros. Se prohíbe el uso de dispositivos extraíbles para la transferencia de información sin autorización previa.

3.7. Todos los archivos deben ser almacenados en repositorios seguros, con acceso controlado y restringido según los niveles de autorización.

3.8. Los documentos innecesarios deben ser eliminados de manera segura, conforme a las normativas internas.

4. MENSAJES ELECTRÓNICOS

Av. Sánchez Carrión Nº 615
Edif. Vértice 22 Oficina 306 - Jesús María - Lima
51-(1) 397 8586 / 51-(1) 957 540 053
arbitraje@cearlatinoamericano.pe
Web: www.cearlatinoamericano.pe

4.1. Todo usuario es responsable del contenido de las comunicaciones que almacene o envíe a través de su cuenta de correo electrónico institucional / WhatsApp Business.

4.2. El correo electrónico institucional / WhatsApp Business debe utilizarse exclusivamente como herramienta de comunicación oficial de la organización.

4.3. El correo electrónico institucional / WhatsApp Business es un medio de intercambio de información estrictamente relacionado con las funciones del cargo. No debe utilizarse para difusión masiva, comunicaciones personales, cadenas de mensajes, esquemas piramidales, contenido terrorista, pornográfico o ilegal, distribución de software pirata, proselitismo político, religioso o racial, amenazas, estafas, virus o código malicioso.

4.4. Los usuarios autorizados no deben enviar mensajes de correo electrónico al exterior de la organización que puedan dañar o comprometer su reputación.

4.5. Bajo ningún motivo se deben abrir o ejecutar correos electrónicos de origen desconocido, ya que podrían contener código malicioso (virus, troyanos, keyloggers, gusanos, etc.), lo que representa un riesgo para los sistemas, programas y datos de la organización.

4.6. Se deben implementar técnicas de prevención para mitigar la recepción de correo spam.

4.7. La organización debe establecer mecanismos de bloqueo para impedir el ingreso y salida de mensajería no autorizada en su red.

4.8. Los servicios de mensajería electrónica deben cumplir con las regulaciones legales vigentes.

4.9. Está prohibido el envío de información confidencial a destinatarios no autorizados o a través de conexiones no seguras.

4.10. Se desaconseja el uso del correo electrónico institucional / WhatsApp Business en redes Wi-Fi públicas o no seguras, debido a los riesgos de interceptación de información.

5. SEGURIDAD DE SERVICIOS DE RED

5.1. Todos los sistemas y servicios de red deben mantenerse actualizados con los parches de seguridad y recomendaciones de los fabricantes, garantizando niveles óptimos de control y protección.

5.2. Se prohíbe a colaboradores y terceros acceder a páginas web que promuevan contenido ofensivo, incluyendo pornografía, violencia, terrorismo, actividades ilegales, discriminación o cualquier otro contenido contrario a las normas de la organización.

5.3. La administración de cuentas de acceso a Internet, correo electrónico y otros servicios de red debe ser realizada exclusivamente por el Área de TI.

5.4. Todos los servicios de red deben contar con mecanismos de detección y eliminación de código malicioso, asegurando la protección contra amenazas digitales.

Av. Sánchez Carrión Nº 615
Edif. Vértice 22 Oficina 306 - Jesús María - Lima
51-(1) 397 8586 / 51-(1) 957 540 053
arbitraje@cearlatinoamericano.pe
Web: www.cearlatinoamericano.pe

5.5. Cada cuenta de correo electrónico debe tener una capacidad de almacenamiento fija, determinada según el rol, funciones, cargo desempeñado o naturaleza del buzón.

5.6. Todos los accesos a la red, tanto internos como externos, deben contar con mecanismos de seguridad perimetral para garantizar su protección.

6. ACUERDOS DE CONFIDENCIALIDAD O NO DIVULGACIÓN

6.1. Para toda contratación, ya sea a plazo fijo o indeterminado, se debe garantizar que el nuevo colaborador firme un acuerdo de confidencialidad, con el fin de proteger los activos de información que maneje. En el caso de terceros contratados por la organización, se deberán establecer acuerdos de servicio de carácter preventivo, asegurando la calidad del servicio recibido y la firma de un convenio de confidencialidad.

6.2. Todo el personal de la organización, independientemente de su modalidad de contrato o formación, así como los terceros vinculados, deben firmar acuerdos o cláusulas en los que se establezca la confidencialidad de la información a la que tengan acceso como consecuencia del desempeño de sus funciones o su relación con la organización.

6.3. La obligación de confidencialidad se mantiene incluso después del cese de la relación contractual o laboral con la organización.

6.4. Divulgación de información del cliente: Se prohíbe totalmente la divulgación de información de clientes a terceros, salvo autorización expresa de la Alta Dirección o cuando sea requerido por autoridades judiciales.

6.5. Divulgación de datos estratégicos de la organización: Se prohíbe a los colaboradores divulgar información sobre la estrategia comercial de la organización, secretos organizacionales, listas de clientes u otra información estratégica. La gestión de estos datos corresponde exclusivamente a los líderes de los procesos estratégicos de la organización.

6.6. Divulgación de información sobre vulnerabilidades del sistema: La información sobre vulnerabilidades del sistema, incluyendo detalles de brechas de seguridad recientes, no debe ser divulgada a personas no autorizadas.

Firmado por la Gerente General: Verónica Sandoval Larraín.

CEAR LATINOAMERICANO S.A.C.
VERONICA SANDOVAL LARRAIN
Gerente General

Av. Sánchez Carrión Nº 615
Edif. Vértice 22 Oficina 306 - Jesús María - Lima
51-(1) 397 8586 / 51-(1) 957 540 053
arbitraje@cearlatinoamericano.pe
Web: www.cearlatinoamericano.pe