POLITICA DE SEGURIDAD DE LA INFORMACIÓN PARA PROVEEDORES

Tabla de Control de Cambios

Versión	Fecha	Razones Generales de Cambios	Autores
1	22/12/2022	▪ Adecuación de la política a las necesidades de Niubiz	– Oliver Palacios – Jaime Rodriguez

Índice

1. Objetivo

Garantizar la protección de los activos de Niubiz que son accesibles por los Proveedores/Terceros.

2. Alcance

Las políticas de seguridad de la información abarcan todos los aspectos administrativos y de control que deben ser conocidos y cumplidos por las jefaturas, todo el personal y terceros que laboren o tengan relación con Niubiz.

3. Definiciones, conceptos y abreviaturas

- **Activo de Información (o Recurso de Información):** Cualquier información o sistema relacionado con el tratamiento de la misma, que tenga valor para la organización.
- **Amenaza (Interna, Externa):** Causa potencial de un incidente no deseado, el cual puede causar daño a un activo de información.
- **Riesgo de la Información:** Probabilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

4. Políticas

4.1 Políticas Generales

1. Todo proveedor que presta servicios a la organización deberá firmar la política PCT-SI-POL-28 Política de Seguridad de la Información para Proveedores, como parte del contrato de servicios.
2. Los proveedores sólo podrán desarrollar para la organización, aquellas actividades cubiertas bajo el correspondiente contrato de prestación de servicios.
3. El proveedor proporcionará los datos completos de la persona de contacto, quien será el encargado de recibir todo tipo de directivas de seguridad de la información. El proveedor proporcionará la relación de personas, perfiles, funciones y responsabilidades asociadas al servicio provisto, e informará puntualmente de cualquier cambio (alta, baja, sustitución o cambio de funciones o responsabilidades) que se produzca en dicha relación.
4. Todo proveedor de servicios deberá velar porque su personal que presta los servicios directamente a la organización cumpla con las políticas de seguridad de la información recogidas en el presente documento. En caso de incumplimiento, la organización se reserva el derecho de solicitar al Proveedor el cambio de personal, sin perjuicio del derecho de la organización de resolver el contrato de prestación de servicios en los términos establecidos en el contrato.
5. El Proveedor deberá garantizar que todo su personal que realiza servicios para la organización cuente con formación y capacitación apropiada para el desarrollo del servicio contratado, tanto a nivel específico en las materias correspondiente a la actividad asociada, como de manera transversal en materia de seguridad de la información.
6. Cualquier tipo de intercambio de información que se produzca entre la organización y el Proveedor se entenderá que ha sido realizado dentro del marco establecido por el contrato de prestación de servicios, de modo que dicha información tendrá el carácter de confidencial y no podrá ser utilizada en ningún caso fuera de dicho marco, ni para fines diferentes a los asociados al contrato.

4.2 Políticas específicas

1. Todo Proveedor que tenga acceso a la información de la organización en ejecución de un contrato de prestación de servicios, deberá considerar que dicha información, es confidencial.
2. Ningún Proveedor podrá utilizar la información de la organización para beneficio propio o de terceros. La información a la que tenga acceso el Proveedor únicamente podrá ser utilizada para los fines específicamente indicados en el contrato de prestación de servicios. Toda información proporcionada por la organización seguirá siendo de propiedad de esta última.
3. El Proveedor garantiza que a la terminación del servicio o ante el pedido efectuado en cualquier momento por la organización, cesará inmediatamente el uso de toda información proporcionada, debiendo entregar, (cualquiera sea el soporte en que se encuentre) toda la información que obre en su poder y destruir toda copia que se haya realizado, entregando una confirmación por escrito de ello con la calidad de declaración jurada.
4. Todas las obligaciones de confidencialidad continuarán vigentes aún culminado el contrato de prestación de servicios por cualquier causa de manera indefinida.
5. Cuando el Proveedor conozca de cualquier pérdida, uso no autorizado o revelación de la Información proporcionada o de propiedad de la organización, deberá comunicarlo inmediatamente, debiendo adoptar todos los pasos necesarios para ayudar a la organización a remediar tal uso no autorizado o revelación de la Información.
6. El proveedor debe garantizar el cumplimiento de las restricciones legales respecto del uso del material protegido por normas de propiedad intelectual.
7. El Proveedor y su personal únicamente podrá utilizar la información y activos tecnológicos autorizados por la organización para el desarrollo de los servicios contratados.
8. La distribución de la información ya sea en formato digital o papel, se realizará mediante los recursos determinados en el contrato de prestación de servicios y para la finalidad exclusiva de facilitar las funciones asociados a dicho contrato.

9. Los recursos que la organización pone a disposición del Proveedor, independientemente del tipo que sean, (informáticos, datos, software, redes, sistemas de comunicación, etc.) están exclusivamente destinados para cumplir con las obligaciones y propósito para los que fueron proporcionados. La organización se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.
10. Se prohíbe expresamente:
    - El uso de recursos proporcionados por la organización para actividades no relacionadas con el propósito de servicio.
    - La conexión a la red de la organización de equipos y/o aplicaciones que no estén especificados como parte del Software propio o bajo supervisión de la organización.
    - Intentar obtener sin autorización explícita otros derechos o accesos distintos a los que la organización haya asignado.
    - Intentar acceder, sin autorización explícita, a áreas restringidas de los Sistemas de Información de la organización.
11. Cualquier persona con acceso a información de la organización deberá respetar al menos las siguientes políticas de escritorio limpio, con el fin de proteger los documentos en papel y dispositivos de almacenamiento removibles y reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo:
    - Almacenar bajo llave los documentos de papel y los medios informáticos con información de la organización en mobiliario seguro cuando no están siendo utilizados.
    - No dejar desatendidos los equipos y bloquear su acceso cuando no estén siendo utilizados.
    - Los listados con datos de carácter personal o información confidencial deberán almacenarse en un lugar seguro al que únicamente tengan acceso personas autorizadas.
    - Para el caso proveedores con asignación de laptops, es obligatorio el uso del candado durante la ausencia de su lugar de trabajo y al cierre de la jornada.
12. Todos los servicios que impliquen accesos a la información o sistemas de información de la organización deberán cumplir con las siguientes políticas con respecto a su personal:
    - El proveedor deberá verificar los antecedentes profesionales, penales y policiales del personal asignado al servicio, garantizando a la organización que en el pasado no haya tenido algún tipo de sanción.
    - El proveedor deberá garantizar a la organización la posibilidad de la baja inmediata del personal asignado al servicio de cualquier persona en relación con la cual la organización le indique.
13. Todo proveedor deberá permitir que la organización lleve a cabo al menos una auditoría de seguridad del servicio al año, colaborando con el equipo auditor y facilitando todas las evidencias y registros que le sean requeridos.
14. El alcance y profundidad de la auditoría será establecido expresamente por la organización en cada caso.
15. El Proveedor deberá ponerse en contacto con el área de Seguridad de la Información de la organización en caso detecte cualquier incidencia relacionada con la información o los recursos de la organización.
16. Todo proveedor de servicios es responsable de transmitir y hacer cumplir las políticas de seguridad de la organización a terceros subcontratados, autorizados debidamente por la organización.

5. Anexos

N/A.