AVISO DE CONFIDENCIALIDAD

"El presente documento es de carácter confidencial. Su lectura está restringida a personal de Netvoice. La distribución o publicación de este documento sin previa autorización está completamente prohibida"

CONTENIDO

POLITICAS DEL SISTEMA DE GESTION DE SEGURIDAD DE INFORMACIÓN DE NETVOICE

Se define la política de Seguridad de Información como:

"Proveer Servicios de Telecomunicaciones gestionando la Seguridad de la Información para prevenir y minimizar el riesgo de incidentes que atenten contra la confidencialidad, integridad y disponibilidad de los activos de información de Netvoice."

Presidencia

POLITICAS DE SEGURIDAD DE INFORMACIÓN

1. Nuestra dirección se compromete a guiar y apoyar la seguridad de la información en las relaciones con: empleados, clientes, proveedores, organismos reguladores y terceros relacionados.
2. Los propietarios de los activos de información deberán velar por la correcta gestión sobre los mismos.
3. Los empleados, contratistas y terceros, deberán entender sus responsabilidades dentro de la seguridad de información y ser los adecuados para los roles asignados.
4. Se debe evitar el acceso físico no autorizado, daño e interferencia a la información y/o servicio.
5. La organización debe operar de forma adecuada y segura los medios de procesamiento, tránsito y almacenamiento de la información y de la prestación de servicio.
6. La organización debe controlar el acceso a la información y los activos, que la procesen, transmitan y/o la almacenen, acorde a los criterios de propiedad, roles y riesgo.
7. La organización debe garantizar que la seguridad sea parte integral de los diferentes sistemas de información y servicios ofrecidos a nuestros clientes.
8. Los incidentes de seguridad que se presenten serán comunicados y tratados de manera que permitan tomar una acción correctiva oportuna.
9. La organización deberá contrarrestar y/o evitar las interrupciones del negocio; protegiendo sus procesos críticos ante convulsión interna y desastres naturales y procurar su reanudación oportuna.
10. La organización evitará las violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad.

NORMATIVAS POR DOMINIO DE SEGURIDAD DE INFORMACIÓN

1. POLÍTICA, ORGANIZACIÓN y RESPONSABILIDADES DE LA SEGURIDAD DE INFORMACIÓN

1.1. La política de seguridad de información debe ser de conocimiento y cumplimiento para todos los empleados de Netvoice S.A.

1.2. Esta política será revisada y actualizada anualmente por parte del oficial de seguridad o en su defecto cuando haya cambiado uno de los objetivos dentro del negocio de la empresa y cuando la situación lo amerite.

1.3. La política de seguridad será explícitamente aprobada por el Gerente General.

1.4. La Gerencia General debe apoyar activamente la seguridad de la información dentro de la organización a través de un compromiso demostrado y la asignación de las responsabilidades de seguridad de la información. Para ello, dentro del presupuesto anual se definirán rubros para la implementación de nuevos proyectos de seguridad de la información que contribuyan al crecimiento organizacional y mejora continua de nuestra red.

1.5. Los Jefes Departamentales serán los responsables de coordinar y organizar las actividades respecto a seguridad de la información en sus departamentos. Entiéndase estas como: preparación para auditorías, manejos de incidencias, reporte de incidencias, tratamiento de incidencias, capacitación, elaboración de procesos, documentos, diagramas, mantenimientos de registros, acciones correctivas, acciones preventivas, revisión y corrección de procesos interdepartamentales, implementación y revisión de controles, medición de indicadores asignados a estos controles. Para esto, los Jefes Departamentales contarán con la asesoría y asistencia del oficial de seguridad de la empresa.

1.6. La organización cumplirá con los requisitos legales establecidos en las leyes ecuatorianas respecto a seguridad de la información. Para esto el departamento legal será el encargado de mantener contacto con las autoridades y estar actualizado con los reglamentos pertinentes.

1.7. Es responsabilidad del representante legal solicitar la firma de un acuerdo de confidencialidad al oficial de seguridad para la realización de sus actividades, el mismo que serán mantenido por el Departamento Administrativo.

1.8. Es responsabilidad de cada Jefe Departamental solicitar la firma de un acuerdo de confidencialidad a todos los empleados y partes externas, los mismos que serán

mantenidos por el Departamento de Recursos Humanos.

1.9. Cada Jefe Departamental será quien analice y evalúe el riesgo ante la contratación de un servicio y defina si es necesario la firma de un acuerdo confidencialidad, en base a las políticas establecidas por el Departamento de Seguridad.

1.10. Todo pasante o cliente que realice actividades dentro de la compañía con el motivo de pruebas de laboratorio o aprendizaje es necesario que firme un acuerdo de confidencialidad mantenido por el Departamento involucrado y copia al Departamento de Recursos Humanos.

2. MANEJO DE INFORMACIÓN

2.1. Todos los documentos de Netvoice S.A son considerados confidenciales (por lo tanto, amparados en los acuerdos de confidencialidad) a excepción de las notificaciones de trabajo a clientes, notificaciones de incidencias, a clientes externos, reportes hacia clientes y publicidad de la compañía.

2.2. Para el tratamiento de la seguridad de la información en las relaciones con los clientes se debe acordar las autorizaciones para actuar ante incidentes de seguridad de información.

3. GESTIÓN ACTIVOS

3.1. El oficial de seguridad debe tener el diagrama de la red y un inventario del direccionamiento público y privado de la empresa, lo cuales deben ser actualizados cada vez que se produzca algún cambio.

3.2. Los Jefes Departamentales serán los responsables de velar por los activos de información que están asignados al departamento a su cargo. En caso de la asignación de un nuevo activo, serán quienes valoren los riesgos relacionados a este activo para su posterior implantación de controles si los resultados lo ameritan. Los Jefes Departamentales recibirán la ayuda del oficial de seguridad en torno a la gestión del riesgo.

3.3. Todos los Jefes Departamentales son los responsables de medir la efectividad de los controles asignados a sus activos u operaciones y deberán reportar cualquier falla del control al oficial de seguridad.

4. RECURSOS HUMANOS

4.1. La implementación, mantenimiento y registro del proceso formal de vinculación, inducción y desvinculación a la compañía será llevado a cabo por el Departamento

Administrativo, y debe contemplar directrices de Seguridad de la información definidas en la empresa.

4.2. Todo incumplimiento de las políticas de seguridad de información de la compañía será sancionado según lo descrito en el reglamento interno de la compañía.

4.3. Los datos personales de los empleados deben ser tratados de forma privada.

4.4. El cumplimiento de políticas y procedimientos de la Seguridad de Información será una de las métricas consideradas en la evaluación anual del personal.

5. SEGURIDAD FÍSICA, AMBIENTAL, DE INSTALACIONES Y MANEJO DE EQUIPAMIENTO

5.1. Todo acceso físico o lógico a la infraestructura en la nube alojada en centros de datos será restringida solo al personal autorizado.

5.2. Todos los empleados debidamente autorizados que ingresen al cuarto de equipos de interconexión deben registrar su entrada y salida en la bitácora respectiva.

5.3. El Jefe Técnico debe velar por el cumplimiento de las buenas prácticas establecidas y mantener una constante retroalimentación con el oficial de seguridad.

5.4. El responsable del activo deberá evaluar la necesidad y frecuencia de mantenimiento del equipo a su cargo para asegurar el buen funcionamiento del mismo, de ser equipo especializado se podrá contar con la ayuda de centros técnicos acreditados para realizar las revisiones y mantenimientos adecuados.

5.5. Queda prohibido que, si existiere pérdida de herramienta o equipo, se compre y reemplace sin conocimiento y autorización de la Gerencia General.

6. SERVICIO DE APOYO

6.1. Toda instalación en las oficinas y nodos deben tener las seguridades eléctricas estandarizadas por el departamento técnico de la empresa.

6.2. Los nodos deben tener respaldos eléctricos como UPS y climatización, de acuerdo a la estandarización definida.

6.3. Las instalaciones de nodos deben contar con supresores de picos y conexión a tierra.

6.4. Los sistemas de climatización, dependiendo de la funcionalidad del sitio en donde se encuentren deberán tener sistemas de encendido automático al momento de regresar la energía eléctrica.

7. SEGURIDAD DEL CABLEADO

7.1. Toda instalación eléctrica deberá ser gestionada por el Departamento Técnico.

7.2. En los nodos, el cableado deberá ser mantenido con orden, limpieza, identificación y colocado dentro de los organizadores de cables.

7.3. Todo deterioro o daño de cableado deberá ser reportado al Departamento Técnico quien a su vez será el responsable de tomar las medidas correctivas y preventivas necesarias.

7.4. Todo cableado en nodos debe cumplir los estándares de cableado definidos por el Departamento Técnico.

8. MANTENIMIENTO DE EQUIPOS

8.1. Todo equipo deberá regirse al manual del fabricante para tomar nota de los mantenimientos recomendados, tanto en periodicidad como en fechas específicas indicadas por el mismo.

8.2. Se debe tener archivadas las garantías de todos los equipos, así como los registros de los mantenimientos para tener un histórico de estos.

8.3. Cuando se requiera dar mantenimiento a cualquier equipo, este debe ser retirado de operación y colocar uno de reemplazo hasta que el primero sea reintegrado a sus labores.

8.4. Los equipos eléctricos de los nodos serán monitoreados dentro de los mantenimientos planificados del departamento técnico.

8.5. Si se tratase de equipo computacional, este deberá ser reportado al jefe inmediato superior para que este contacte al Jefe de Sistemas, para que proceda con la revisión y solución del problema presentado, en caso de ser necesario que indique si el equipo debe ser cambiado para que el jefe tramite el cambio del mismo.

9. SEGURIDAD DE EQUIPOS FUERA DE LAS INSTALACIONES DE LA ORGANIZACIÓN

9.1. Todo equipo que se retire de las instalaciones de la empresa deberá contar con su respectiva orden de salida de equipos debidamente autorizada por el responsable administrativo.

9.2. Ningún equipo de trabajo debe ser dejado sin observación mientras se encuentre fuera de las instalaciones de la empresa.

9.3. El custodio del equipo es el responsable de su transporte seguro.

9.4. Cuando se deba trabajar en sitios poco seguros de la ciudad o campo, se deberá solicitar al departamento administrativo que proporcione resguardo para trabajar en el sitio.

10. SEGURIDAD EN LA REUTILIZACIÓN O ELIMINACIÓN DE EQUIPOS

10.1. Todos los servidores de la infraestructura crítica en los centros de datos deberán ser respaldados regularmente. Los respaldos no podrán ser almacenados en la misma ubicación en donde se encuentran los servidores que se respaldan.

10.2. Cuando los equipos deban ser dados de baja por cualquier razón y los mismos tenga discos o medios de almacenamiento, estos deben ser formateados de manera segura. Si el disco o el medio de almacenamiento no puede ser formateado, este deberá ser destruido.

10.3. Todos los equipos que se den de baja deberán cumplir con las políticas administrativas y de auditoría para la eliminación de activos de información de la empresa.

11. RETIRO DE LA PROPIEDAD

11.1. Solo personal autorizado puede sacar equipos de cómputo con información de la empresa, acorde a sus áreas de trabajo.

11.2. Todo el personal debe cumplir las disposiciones dadas por la Jefatura de Sistemas en cuanto a encriptación de información en el disco duro.

11.3. Toda instalación de software deberá ser autorizada la Jefatura de Sistemas.

11.4. Cuando se trate de software administración de sistemas, éstos deberán estar bajo custodia del departamento que los utiliza y como protección deberán ser archivados en un servidor de la empresa.

12. GESTIÓN DE CAMBIO

12.1. Todo cambio en la red deberá ser revisado y aprobado por la Jefatura Técnica.

12.2. Queda estrictamente prohibido a cualquier departamento instalar elementos o equipos de red dentro de la red interna sin previa autorización de la Jefatura Técnica.

12.3. Todos los trabajos programados deben quedar registrados en la bitácora de mantenimiento y deben ser autorizados y cumplir con las políticas y lineamientos establecidos por la Jefatura Técnica.

12.4. Todo trabajo que pueda tener afectación a clientes debe tener la autorización de la Jefatura Técnica.

12.5. Los trabajos de acción correctiva deben ser aprobados por la Jefatura Técnica.

13. SEPARACIÓN DE LOS RECURSOS PARA EL DESARROLLO, PRUEBA/ENSAYO Y OPERACIÓN

13.1. Para todos los proyectos se debe proporcionar mínimo dos ambientes de trabajo que son: desarrollo y producción.

13.2. No se debe cambiar ninguna configuración, versión de sistema operativo, arquitectura de red, etc., sin realizar las pruebas en el ambiente de desarrollo.

13.3. Los desarrollos probados serán puestos en producción con el visto bueno de la Jefatura de Sistemas.

13.4. Los equipos del ambiente de desarrollo deberán tener claves de acceso diferentes a los de ambiente de producción. Las claves deberán cumplir la política de clave segura.

14. TRATAMIENTO, MONITOREO y ENTREGA DE SERVICIO DE TERCERAS PARTES

14.1. Se deberán realizar acuerdos de confidencialidad y/o no divulgación con los proveedores que puedan tener acceso a información confidencial de la empresa o información personal de clientes o empleados.

14.2. Linkotel deberá solicitar a sus proveedores los pormenores del servicio entregado, tales como procedimientos de control de cambios, diagramas técnicos del servicio o producto, mecanismos de continuidad del servicio, procedimiento de apertura de tickets, niveles de escalamiento y en general todo lo necesario para garantizar que el servicio del proveedor cumple con los requisitos definidos en el contrato.

14.3. Linkotel debe exigir a sus proveedores una política de control de cambios debidamente documentada. Esta información debe ser solicitada por la Jefatura Técnica y/o Jefatura de Sistemas, según aplique.

14.4. El Área de Infraestructura deberá monitorear proactivamente si el proveedor ha realizado algún cambio notificado o sin notificación e informar la Jefatura Técnica el detalle de los cambios.

15. GESTIÓN DE LA CAPACIDAD

15.1. La responsabilidad de la Gestión de la Capacidad de la infraestructura crítica será de Jefatura Técnica. La Jefatura Técnica y la Jefatura de Sistemas deberán monitorear la capacidad, y de ser el caso, solicitar la provisión de capacidad para su aprobación por parte de la Gerencia General.

16. POLÍTICA DE ACEPTACIÓN DEL SISTEMAS DE SOFTWARE

16.1. Toda aceptación de un nuevo sistema ya sea que provenga del interior de Linkotel o de un proveedor externo, deberá pasar por una etapa de pruebas antes de ser colocado en producción. La Jefatura de Sistemas revisará y autorizará la puesta en producción de sistemas de información, configuraciones, servicios, bases de datos y servidores.

16.2. Cualquier otro nuevo sistema debe ser normado según los requerimientos de seguridad de la información (confidencialidad, integridad y disponibilidad), los cuales debe ser establecidos previos al inicio del proyecto. Los requisitos de seguridad de la información serán revisados por la Jefatura de Sistemas y aprobados por la Gerencia General.

17. DOCUMENTACIÓN DE SISTEMAS

17.1. Los manuales de usuario son de acceso público para personal de la empresa.

17.2. Los manuales técnicos son de acceso restringido para el área de técnica.

18. SISTEMA DE INFORMACIÓN

18.1. Todo sistema de información interno debe ser accedido por el personal autorizado con usuarios nominales para cada sistema.

18.2. Toda información que almacenen, transmita o procesen los sistemas internos de Linkotel es de carácter confidencial.

18.3. El manejo de la información dentro del sistema dependerá de los perfiles de acceso asociados a los usuarios.

18.4. El número de cuenta principal (PAN) del tarjetahabiente deberá ser cifrada en todos los medios de transmisión y almacenamiento incluyendo bases de datos. En los casos de ser requerida la presentación o visualización de los datos sensibles se seguirá el principio de necesidad del saber de acuerdo a las funciones del personal; por defecto se ocultará la información y solo se presentarán los primero 6 dígitos o los últimos 4 dígitos del PAN.

18.5. Todo acceso privilegiado que descifre los datos cifrados en las bases de datos debe ser registrado.

18.6. El acceso a sistemas internos a través de redes públicas se realizará por un canal seguro que cifre la información.

18.7. Todos los accesos de usuarios con acceso privilegiado a través de cualquier aplicación deben quedar registrada en el sistema de logs.

18.8. Personal autorizado por la Gerencia General podrá acceder a los logs para fines de investigación o seguimiento de control de acceso por solicitud de la Jefatura de Sistemas.

18.9. De acuerdo a la política de confidencialidad de la empresa, la información obtenida de los registros de logs es de propiedad de la empresa. Sólo la Gerencia General podrá autorizar la liberación de esta información al público o a clientes.

18.10. El Jefe Administrativo notificará la salida del personal a la Jefatura de Sistemas que se encargará de deshabilitar los accesos en los diferentes sistemas, bases de datos y equipos que el personal saliente tenía acceso o en custodia.

18.11. Todo análisis de un incidente de seguridad deberá estar basado en la información de los logs o registros de acceso. Con el resultado del análisis se deberán tomar las acciones correctivas y preventivas apropiadas.

18.12. Todos los servidores de la infraestructura crítica, logs y registros de acceso deben estar sincronizados en tiempo.

18.13. En la adquisición y/o desarrollo de cualquier sistema de información de Linkotel debe incluirse los requisitos mínimos de seguridad, para lo cual es necesario seguir las funciones de seguridad definidas por la Jefatura de Sistemas junto con la aprobación de la Gerencia General.

19. CONTROL DE ACCESOS

19.1. El acceso a los servidores de la infraestructura crítica por parte de proveedores o terceros relacionados deberá ser autorizado por la Jefatura Técnica. Estos accesos deberán emplear utilizar métodos de conexión cifrada (por ejemplo, uso de VPN).

19.2. Deberá mantenerse un registro de acceso y de las actividades realizadas.

19.3. Para obtener el acceso a los sistemas internos, el jefe de área deberá solicitar a la Jefatura de Sistemas el tipo de acceso y las aplicaciones. El acceso deberá ser autorizado por la Gerencia General.

19.4. Los cambios en los privilegios de acceso de un usuario deberán ser solicitado por el jefe del Área correspondiente a la Jefatura de Sistemas. El cambio deberá ser autorizado por la Gerencia General.

20. USO DE CONTRASEÑAS

20.1. El usuario y clave proporcionados son de uso personal e intransferible, por lo tanto, el dueño del mismo será responsable precautelar su buen uso en los equipos, sistemas, aplicaciones y bases de datos.

20.2. La política de clave segura aplicable a las credenciales de acceso a sistemas, equipos, bases de datos y aplicaciones es de que las claves tengan un mínimo de 8 caracteres que incluyan los siguientes grupos: letras mayúsculas, letras minúsculas, números y símbolos.

20.3. Las claves de acceso de los servidores de la infraestructura crítica deberán cambiarse al menos cada seis por parte del dueño de los activos.

20.4. Ningún equipo, sistema operativo, base de datos y aplicativos en producción deberá mantener las contraseñas por defecto del fabricante.

20.5. Las contraseñas de los números de teléfono asignadas a los clientes deberán cumplir la política de clave segura.

21. PROCEDIMIENTOS DE CONEXIÓN SEGURA

21.1. Los accesos a todos los sistemas operativos deberán hacerse a través de métodos criptográficamente seguros y que empleen al menos un factor de autenticación.

21.2. Todos los sistemas operativos deben bloquear las sesiones inactivas por un tiempo de 5 minutos.

22. TRABAJO A DISTANCIA

22.1. Los empleados de Linkotel podrán conectarse a la red interna previa autorización del oficial de seguridad informática solo para realizar labores relativas a sus funciones.

23. PROCESAMIENTO CORRECTO DE LAS APLICACIONES

23.1. Las aplicaciones antes de entrar a producción deben pasar por el procedimiento establecido por la Jefatura de Sistemas.

24. CÓDIGO FUENTE

24.1. Todo código fuente desarrollado es de propiedad exclusiva de Linkotel.

24.2. El acceso a los servidores de aplicaciones debe permitir acceso únicamente a personal del Departamento de Sistemas desde direcciones IP específicas.

24.3. Todos los empleados del departamento de sistemas deben almacenar el código fuente en un servidor que se encuentre controlado su acceso.

24.4. El Jefe de Sistemas será el encargado de definir las políticas de desarrollo seguro para las aplicaciones.

25. TRATAMIENTO DE INCIDENCIAS

25.1. Todos los empleados de Linkotel S.A. están en la obligación de reportar cuando se encuentre una debilidad y/o incidente de la seguridad de la información.

25.2. El tratamiento de vulnerabilidades y/o incidentes debe ser registrado con su respectiva acción correctiva.

25.3. El tratamiento de incidentes siempre debe estar orientados a la solución de la causa raíz de problema. Salvo excepciones donde ya no dependa de la organización dicha causa.

26. PLAN DE CONTINUIDAD DEL NEGOCIO

26.1. La implantación, prueba y mejoramiento de un Plan de Continuidad del Negocio será responsabilidad del Jefe Técnico y de la Gerencia General. Las pruebas del mismo se deben realizar en ambientes controlados mínimo una vez por año.

26.2. La reevaluación de los planes de continuidad del negocio se lo realizará cada año o en su defecto cuando un cambio considerable de la infraestructura lo exija.

26.3. Se deberán realizar simulacros de falla de la red o sistemas periódicamente con la finalidad de entrenar al personal de soporte para mejorar sus tiempos de respuesta, así como también para detectar cualquier falla no contemplada en trabajos previos y/o cualquier error en los procedimientos.

27. CUMPLIMIENTO

27.1. El Departamento de Sistemas será el encargado de comprobar el cumplimiento técnico de los sistemas acorde a las normas de seguridad de información.

APROBACIÓN

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Ing. Roberto Ruiz	Ing. Francisco Estupiñán Abg. Gregorio Zambrano	Pablo Baquerizo

CONTROL DE CAMBIOS

Control de Cambios:

12/08/2019
- Política de seguridad original.

14/08/2019
- Aprobación