Política de Seguridad de la Información

GERENCIA DE TELECOMUNICACIONES Y CIBERSEGURIDAD

AGOSTO 2020

Contenido

1.	**INTRODUCCIÓN**	**3**
2.	**OBJETIVOS**	**3**
3.	**ALCANCE**	**4**
4.	**ÁMBITOS Y DOMINIOS**	**5**
5.	**ROLES Y RESPONSABILIDADES**	**7**
6.	**DIRECTRICES**	**7**
7.	**CUMPLIMIENTO**	**8**
8.	**REFERENCIAS**	**9**

1. Introducción

NetMetrix una empresa de Gestión Avanzada de Redes formada por un grupo de ingenieros especialistas en TI, Redes y Comunicaciones con más de 30 años de experiencia en diseño, operación y venta de soluciones integradas TIC. Dentro del compromiso que hemos asumido de cara a la gestión de la seguridad se ha establecido una política general de seguridad, incorporado las mejores prácticas de seguridad basados en ISO 27001 y NIST, política que es revisada y aprobada por la Gerencia General regularmente con miras a cumplir los requerimientos específicos de seguridad. Cumplir estos estándares de seguridad nos permite proteger nuestros activos de amenazas, cumplir normas y regulaciones vigentes, resguardar nuestra reputación empresarial respondiendo así a la confianza de nuestros clientes.

La política de seguridad de la información tiene un enfoque en los siguientes ámbitos:

- Seguridad organizacional.
- Seguridad de la infraestructura física.
- Seguridad de la infraestructura tecnológica.
- Ciberseguridad.
- Seguridad de la información.
- Seguridad de los datos.
- Seguridad de los servicios provistos a clientes.

2. Objetivos

El objetivo general es nuestro compromiso con la seguridad y resguardo de los activos, su uso y buenas prácticas relacionadas con la mantención de la integridad, confidencialidad y disponibilidad de dichos activos. Proteger la confidencialidad, integridad y disponibilidad de la información es nuestro objetivo estratégico, razón por la que se establecen los siguientes objetivos específicos.

a) Definir los requisitos de seguridad de la organización que permiten asegurar la confidencialidad, integridad y disponibilidad de nuestros activos de información.
b) Establecer e implementar controles de seguridad, con el objeto de resguardar los activos y garantizar que los objetivos y estrategias definidas.
c) Cumplir con la normativa vigente referente a la seguridad, a fin de minimizar los riesgos e impactos económicos y reputacionales.
d) Monitorear y revisar la gestión de seguridad a intervalos planificados, con el objeto de asegurar la mejora continua.

e) Mantener identificado todos los activos de información relevantes presentes directa o indirectamente en cada proceso y servicio de la organización, en cada uno de los ámbitos definidos.
f) Realizar las actividades necesarias de gestión de riesgos para diseñar e implementar medidas y controles que permitan mitigar los riesgos que sean identificados, sin perder de vista el enfoque de la gestión estratégica de seguridad.
g) Mantener una estructura y un marco de políticas, normas, estándares, certificaciones y procedimientos en materia de seguridad.
h) Capacitar a los empleados acerca de su responsabilidad en el logro de los objetivos de seguridad fijados y de la incorporación progresiva de buenas prácticas relacionadas con ello.
i) Generar conciencia y establecer una cultura de seguridad para nuestros empleados y colaboradores, promover la comprensión de las responsabilidades individuales relacionadas con el alcance definido.
j) Proveer seguridad a los elementos informáticos y de comunicaciones donde se almacene, procese y trasmita información propia o de nuestros clientes.
k) Generar capacidades para responder frente a ataques y amenazas de perdida de información.
l) Resguardar los recursos tecnológicos, de comunicaciones e información, por medio de la implementación de medidas de control de acceso, de modo de garantizar que tales activos son accesibles por personas, medios y fines autorizados.
m) Fortalecer por medio del desarrollo de políticas, directrices, normas y procedimientos de seguridad, que la confidencialidad, integridad y disponibilidad esté de acuerdo con los niveles de criticidad, clasificación, inversión, y las necesidades de la empresa y sus clientes.
n) Proveer los recursos humanos, técnicos, financieros necesarios para sustentar esta política. Lo anterior, permitirá dar un marco regulatorio que proporcione principios generales para identificar, proteger, detectar, responder y recuperar los activos frente a los riesgos asociados a la seguridad.

3. Alcance

En base a las necesidades detectadas y en conjunto con los requerimientos de las partes interesadas se han definido los siguientes ámbitos de trabajo:

- Seguridad organizacional
- Seguridad de la infraestructura física
- Seguridad de la infraestructura tecnológica
- Seguridad de la información y los datos propios y de nuestros clientes
- Ciberseguridad
- Seguridad de los servicios provistos a clientes

4. Ámbitos y Dominios

a) GOBIERNO Y ORGANIZACIÓN DE LA SEGURIDAD

Para la administración de la seguridad, se debe contar con un encargado de seguridad dedicado al logro de los objetivos expresados en esta política. Para ello, se define una estructura organizacional y de gobierno, con dependencia funcional y roles claramente establecidos.

b) SEGURIDAD ORGANIZACIONAL Y DE LAS PERSONAS

Debido a que una parte significativa de los problemas en la seguridad puede ser causado por empleados descuidados, mal informados, o disgustados, se hace necesario el definir e implantar mecanismos para la creación de un ambiente de trabajo adecuado

c) GESTIÓN DE ACTIVOS

Todos los activos deben ser inventariados y controlados de manera apropiada. Esto se aplica a los recursos físicos y lógicos dentro de los ámbitos definidos. Estos recursos son cruciales para el éxito del negocio y se deben proteger por medio de controles apropiados para reducir al mínimo cualquier riesgo que los pueda afectar.

d) CONTROL DE ACCESO

Nuestros activos son esenciales, por lo que el acceso a todos los activos debe ser concedido de una manera controlada y periódicamente monitoreada. El protocolo definido en este aspecto es prohibir estrictamente el acceso a menos que sea concedido en forma explícita, y de acuerdo con las necesidades de conocer de las diferentes partes interesadas.

e) CRIPTOGRAFÍA

La información confidencial de la empresa y sus clientes debe ser resguardar de accesos no autorizados mediante de la implementación de controles criptográficos aplicables a la transmisión y almacenamiento de datos sensibles.

f) SEGURIDAD FÍSICA Y AMBIENTAL

Las medidas de seguridad físicas deben estar operativas para resguardar la seguridad y la integridad de las personas y de nuestras oficinas. Las medidas de protección deben estar de acuerdo con la clasificación de los activos y a la información procesada, almacenada, y manejada internamente.

g) ADMINISTRACIÓN DE OPERACIONES

Se deben desarrollar e implementar requerimientos de seguridad para mantener el control sobre las operaciones. Con este objeto se deben definir e implementar las métricas de control adecuadas e incorporar sistemas de monitoreo continuo sobre la operación de seguridad. Lo anterior permite identificar, detectar y prevenir oportunamente los riesgos y

amenazas de origen interno o externo que pueden comprometer la seguridad, continuidad y/o la ciberseguridad de los servicios.

h) ADMINISTRACIÓN DE COMUNICACIONES

La administración de las comunicaciones se debe estructurar de modo tal de asegurar que los datos que se transmiten por las redes de comunicaciones se encuentren adecuadamente protegidos. Para ello se deben establecer controles técnicos y de gestión que garanticen un nivel de resguardo acorde a la criticidad de los datos.

i) DESARROLLO, MANTENCIÓN E IMPLEMENTACIÓN DE SISTEMAS

El diseño de la infraestructura y la implementación de aplicaciones de negocios deben cumplir formal y explícitamente todos los requerimientos de seguridad definidos. Estos requerimientos deben ser incorporados en cada paso del ciclo de diseño, desarrollo e implementación de productos, servicios y sistemas.

j) RELACIÓN CON PROVEEDORES

Se debe asegurar que el proceso de gestión de proveedores incorpora el cumplimiento de los lineamientos de seguridad, con el objeto de garantizar que los servicios brindados por estos cubren las necesidades de la organización en cuanto a la seguridad y resguardo de activos propios y de nuestros clientes.

k) RESPUESTAS A INCIDENTES

Se debe asegurar que los eventos e incidentes de seguridad sean notificados de forma adecuada y oportuna a los responsables de los activos, con el propósito evaluar el incidente para mitigar los riesgos asociados y responder adecuadamente a estos incidentes en el futuro. Lo anterior de acuerdo con los más altos estándares internacionales tales como NIST y el conjunto de normas ISO 27000.

l) ADMINISTRACIÓN DE LA CONTINUIDAD DEL NEGOCIO

Se debe disponer de un sistema de administración para asegurar la continuidad de la seguridad y la recuperación rápida ante incidentes o interrupciones inesperadas de los servicios. El plan de continuidad del negocio debe incluir procesos y procedimientos de recuperación ante cualquier interrupción del servicio.

m) CUMPLIMIENTO

Se debe cumplir con todas las reglas y regulaciones aplicables por la ley, en lo que respecta a resguardo de información. Esto incluye aspectos penales o civiles, estatutos, reglamentos u obligaciones contractuales. Satisfacer los requerimientos de seguridad incorporado en las leyes, así como la protección de la información propia y/o datos de colaboradores, clientes y proveedores.

5. Roles y Responsabilidades

Contamos con una estructura de gobierno y de gestión de la seguridad en base a tres niveles:

- Un **nivel estratégico** donde se establecen, coordinan y aprueban los lineamientos generales y la estrategia de seguridad, proveyendo los recursos humanos, tecnológicos y financieros requeridos para alcanzar los objetivos de la presente política.
- Un **nivel táctico** donde se definen, priorizan y evalúan los proyectos, riesgos e iniciativas de seguridad en cada uno de los ámbitos antes mencionados.
- Un **nivel operacional y de gestión** donde se implementan, controlan y supervisan los indicadores principales de la seguridad que permiten visualizar oportunamente los riesgos y amenazas en cada uno de los ámbitos de la política, de manera de responder adecuadamente ante incidentes de seguridad.

Todos nuestros colaboradores participan activa y responsablemente, cada uno desde su función específica, en la mantención de la seguridad de la compañía.

6. Directrices

NetMetrix asume los siguientes compromisos de actuación en materia de seguridad y privacidad:

a) La seguridad de las personas es el bien más valioso.

b) Los bienes físicos como instalaciones administrativas y la infraestructura física de la red deben ser protegidos contra los riesgos de naturaleza, actos deliberados y aquellas amenazas que pongan en riesgo los activos que soportan y contienen.

c) La información y los sistemas de información son activos valiosos y deben ser protegidos contra amenazas o riesgos internos y externos, para resguardar su disponibilidad, integridad y confidencialidad.

d) La ciberseguridad es una función clave para proteger los activos ante los riesgos del ciberespacio.

e) La seguridad de los activos es responsabilidad de todos nuestros colaboradores, independientemente del cargo que desempeñan.

f) Todo colaborador debe acceder exclusivamente a la información que le sea estrictamente necesaria para cumplir sus funciones.

g) Todo colaborador tiene la obligación de notificar cualquier actividad o situación que afecte o pueda afectar la seguridad de los activos o dependencias.

h) Netmetrix reconoce que la sensibilización, capacitación y entrenamiento adecuados a su personal en las materias de seguridad, son tareas prioritarias y recurrentes.

i) Se establece un conjunto de políticas, planes y procedimientos de seguridad en materias específicas, las cuales forman parte integral de la presente política.

j) El Comité de Seguridad es responsable de entregar direccionamiento en los temas de seguridad y tiene la autoridad para su implementación, control y seguimiento para garantizar la mejora continua en materias de seguridad.

k) Se debe velar por la difusión de las políticas de seguridad.

l) El incumplimiento de las políticas de seguridad, constituyen una falta y serán sancionadas en conformidad a lo establecido en el reglamento interno.

m) Adherimos las mejores prácticas de seguridad, como marcos de referencia internacionales para la gestión de los riesgos de la seguridad y su mejora continua.

n) Declaramos la decisión de cumplir con la legislación y normativa vigente en temas de seguridad y privacidad de los datos.

7. Cumplimiento

La adecuada implementación y articulación de esta Política debe ser auditada periódicamente tanto en sus alcances técnicos u organizacionales. Los hallazgos detectados deben ser informados a las áreas respectivas para su pronta solución.

Infracciones al cumplimiento de esta Política serán tratadas de acuerdo con el Reglamento Interno de trabajo y de acuerdo con las definiciones del Manual de Buenas Prácticas Empresariales o Código de Ética.

8. Referencias

La presente política se sustenta considerando la aplicación de las mejores prácticas de seguridad:

- ISO/IEC 27001:2013 Information security management systems
- ISO/IEC 27002:2013 Code of practice for information security controls
- ISO/IEC 31000:2018 Risk Management
- ISO/IEC 27035:2016 Information security incident management
- ISO/IEC 27701:2019 for privacy information management
- ISO/IEC 27017:2015 Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2019 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- NIST Cybersecurity Framework (CSF) v1.1
- Reglamentos y normativas emanadas por entidades regulatorias locales.
- Reglamento Interno de Orden, Higiene y Seguridad.
- Manual de Buenas Prácticas Empresariales o Código de Ética.
- Manual de Prevención de Delitos.

La presente Política de Seguridad ha sido revisada y aprobada por el Comité de Seguridad de NetMetrix con fecha 10 de Agosto de 2020, fecha a partir de la cual inicia su vigencia. Se procederá con su revisión al menos una vez al año, pudiendo ser modificada en cualquier momento, de acuerdo con las necesidades de la empresa.