





Norma de Seguridad en Telecomunicaciones

Versión: 2.1

Confeccionó	Revisó	Aprobó
BDO Consultoría Externa	 Carla Leiva - CISO	 Francisco Canale - Director

NORMA DE SEGURIDAD EN TELECOMUNICACIONES	intiza
	Clasificación: Restringida
Tipo: Norma	Fecha vigencia: 30/12/2024
Código: NO-SI-23- Seguridad en Telecomunicaciones	Versión: 2.1

Contenido

1. Objetivo	3
2. Alcance	3
3. Responsabilidades	3
4. Desarrollo	4
4.1. Conexiones externas	4
4.2. Firewalls	4
4.3. Gestión de Cambios en el Firewall	5
4.4. Auditoría y monitoreo de Telecomunicaciones	5
5. Referencias	6
5.1. Normativa Relacionada	6
5.2. Definiciones	6
6. Historial de Versiones	7

NORMA DE SEGURIDAD EN TELECOMUNICACIONES	intiza
	Clasificación: Restringida ▾
Tipo: Norma	Fecha vigencia: 30/12/2024
Código: NO-SI-23- Seguridad en Telecomunicaciones	Versión: 2.1

1. Objetivo

Definir las pautas generales de seguridad en el diseño e implementación de redes de computadoras e identificar las zonas que la componen, en función de los servicios e información que se ofrecen o exponen en cada una de ellas, y la posibilidad de acceder a esas redes desde otras zonas o redes, con el propósito final de evitar exposición o acceso potencial a personas y/o partes no autorizadas, asegurando así una adecuada protección de la información en los procesos de transmisión y recepción de datos.

2. Alcance

La presente Norma se aplica a la totalidad de los componentes de red administrados por INTIZA, incluyendo, pero no limitados a, firewall, routers y switches y puntos de acceso inalámbrico.

3. Responsabilidades

Tecnología revisará anualmente esta Norma y/o realizará los ajustes necesarios cuando la misma así lo requiera.

En particular, y con el fin de llevar adelante una administración lógica de los componentes de red de la compañía, **Tecnología** tomará las siguientes funciones y responsabilidades generales:

- Administrar y supervisar la operación segura de todo el hardware y el software relacionado con las comunicaciones.
- Supervisar el mantenimiento seguro y eficiente de las redes de comunicaciones.
- Monitorear la performance y rendimiento de las redes, incluidos sus componentes.
- Comprobar que los periféricos funcionan correctamente.

NORMA DE SEGURIDAD EN TELECOMUNICACIONES	intiza
	Clasificación: Restringida
Tipo: Norma	Fecha vigencia: 30/12/2024
Código: NO-SI-23- Seguridad en Telecomunicaciones	Versión: 2.1

4. Desarrollo

4.1. Conexiones externas

Todas las conexiones externas a la red de INTIZA deben cumplir las siguientes consideraciones:

- Todo acceso externo debe realizarse a través de Redes Privadas Virtuales (VPN).
- Todos los accesos externos deben ser autorizados y registrados a fin de determinar posibles intentos de acceso no autorizados.
- La administración de los dispositivos de comunicación debe realizarse a través de un protocolo seguro.

Se deben utilizar sistemas de detección de intrusiones (IDS o IPS) que permitan la detección de posibles ataques perpetrados en las conexiones externas. Verificar que la configuración generará alertas al personal. Seguridad de la Información debe tomar las medidas adecuadas para prevenirlos.

4.2. Firewalls

Se deben definir los estándares técnicos mínimos de seguridad a utilizar en la selección e implementación de los firewalls aprobados y la protección del perímetro.

Se debe controlar que se mantenga actualizado el software correspondiente a los firewalls basándose en las recomendaciones del proveedor de dichos productos, a fin de minimizar las vulnerabilidades potenciales.

El responsable de Seguridad de la Información debe realizar una revisión al menos semestral de las reglas implementadas.

Se deben emplear los firewalls para realizar una inspección de la capa de aplicación de los protocolos considerados críticos para el ambiente protegido.

NORMA DE SEGURIDAD EN TELECOMUNICACIONES	intiza
	Clasificación: Restringida
Tipo: Norma	Fecha vigencia: 30/12/2024
Código: NO-SI-23- Seguridad en Telecomunicaciones	Versión: 2.1

4.3. Gestión de Cambios en el Firewall

Seguridad de la Información deberá evaluar el impacto potencial de cualquier cambio en el Firewall antes de aprobarlo. La evaluación del impacto debe ser llevada a cabo en base al daño potencial a la confidencialidad, integridad y disponibilidad de la información que se procesa como consecuencia del cambio.

En los casos que los cambios en el Firewall impliquen un riesgo a la seguridad de INTIZA, se deberá dar participación e informar a la Gerencia para que asuma el riesgo de dicho cambio o rechace la solicitud.

Antes de que un firewall se utilice en Producción, se deberá considerar la existencia de controles de seguridad, lineamientos y procedimientos de operación aplicables.

Se deberá contar con controles sobre los cambios en las reglas de los firewalls, los cuales se deberán documentar.

4.4. Auditoría y monitoreo de Telecomunicaciones

Se deberá definir la información que se mantendrá en los registros de auditoría de los firewalls, con el objetivo de detectar y registrar actividad sospechosa. Se deberá incluir información necesaria para permitir la identificación del origen y destino y el tipo de actividad realizada.

Los registros de auditoría deben ser mantenidos en línea por un mínimo de 3 (tres) meses. Los registros de auditoría archivados se deben mantener durante 6 (seis) años como mínimo y se los debe guardar como una copia de seguridad por separado para que sean fáciles de recuperar en caso de necesitarlos.

Los registros del firewall deben revisarse al menos cada 6 (seis) meses para determinar si se han detectado ataques.

Las reglas configuradas en firewalls, deberán revisarse al menos cada 6 (seis) meses.

NORMA DE SEGURIDAD EN TELECOMUNICACIONES	intiza
	Clasificación: Restringida
Tipo: Norma	Fecha vigencia: 30/12/2024
Código: NO-SI-23- Seguridad en Telecomunicaciones	Versión: 2.1

5. Referencias

5.1. Normativa Relacionada

Categoría	Título	Código
Normativa Interna	Gestión de Cuentas de Usuarios	NO-SI-02

5.2. Definiciones

Término	Descripción
Firewall	Programa informático que controla el acceso de una computadora a la red y de elementos de la red a la computadora, por motivos de seguridad.
Routers	Es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función es la de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.
Telecomunicaciones	Las telecomunicaciones son la transmisión a distancia de datos de información por medios electrónicos y/o tecnológicos.

6. Historial de Versiones

Versión	Fecha	Resumen de Cambios
---------	-------	--------------------

Este documento es propiedad exclusiva de INTIZA y su reproducción total o parcial está totalmente prohibida. El uso, copia, reproducción o venta de esta publicación, sólo podrá realizarse con autorización expresa y por escrito del propietario de la publicación. La versión impresa de este documento pierde automáticamente su vigencia.

NORMA DE SEGURIDAD EN TELECOMUNICACIONES	intiza
	Clasificación: Restringida
Tipo: Norma	Fecha vigencia: 30/12/2024
Código: NO-SI-23- Seguridad en Telecomunicaciones	Versión: 2.1

1.0	21/01/2022	Creación de la norma de Seguridad en Telecomunicaciones.
1.0	24/06/2022	Aprobado por Comité de Dirección: MI-DI-05- Minuta de Comité de Dirección N° 5.
2.0	10/08/2022	Se revisó contenido y se hicieron ajustes en el mismo.
2.0	11/10/2022	Aprobado por Comité de Dirección: MI-DI-06- Minuta de Comité de Dirección N° 6.
2.1	30/12/2024	Se realizan cambios en el formato del documento, no en su contenido ya que el mismo sigue vigente.
2.1	30/12/2024	Aprobado por Comité de Dirección.