intiza

Norma de Seguridad Cloud

Versión: 1.0

Confeccionó	Revisó	Aprobó
BDO - Consultoría externa	 Carla Leiva	 Francisco Canale - Director

NORMA DE SEGURIDAD CLOUD	intiza Clasificación: Restringida
Tipo: Norma	Fecha vigencia: 03/01/2025
Código: NO-SI-27- Seguridad Cloud	Versión: 1.0

Contenido

1. Objetivo

El objetivo del documento es establecer lineamientos, directrices y medidas de seguridad necesarias para el uso seguro, eficiente y responsable de los servicios en la nube a fin de proteger los datos y la seguridad de la información.

2. Alcance

Esta norma se aplica a todos los empleados, contratistas y terceros que utilicen servicios en la nube en nombre de INTIZA.

3. Responsabilidades

Seguridad de la Información será responsable de asegurar que la presente norma sea implementada y se cumpla.

Tecnología será responsable de implementar y mantener las medidas establecidas en la presente norma.

Todos los **colaboradores** serán responsables de reportar cualquier incidente de seguridad o vulnerabilidad encontrada.

4. Desarrollo

Los servicios en la nube deben ser contratados a proveedores confiables que cumplan con los estándares de seguridad y privacidad. Se debe revisar que el acuerdo de servicio en la nube aborde los requisitos de confidencialidad, integridad, disponibilidad y gestión de la información de la organización.

El uso de servicios en la nube implica la responsabilidad compartida de la seguridad de la información entre el proveedor de servicios en la nube e INTIZA. No obstante, INTIZA es el principal responsable de la seguridad de la información almacenada, transmitida y procesada en su entorno cloud, por lo tanto, deberá conocer e implementar los parámetros de seguridad necesarios para proteger la misma.

4.1. Seguridad de los datos

Se deben implementar medidas de control para restringir el acceso a los datos almacenados en la nube. Estos controles deben estar basados en roles asegurando que solo el personal autorizado tenga acceso a recursos específicos, de acuerdo a los lineamientos establecidos en la norma de **Gestión de Cuentas de Usuarios.**

Todos los accesos a servicios en la nube deben realizarse utilizando un segundo factor de autenticación (MFA) y contar con contraseñas fuertes que cumplan con los lineamientos descriptos en la norma de **Gestión de Contraseñas.**

Los datos confidenciales o sensibles deben ser cifrados antes de ser almacenados en la nube, utilizando protocolos seguros tanto para los datos en reposo, como para datos en tránsito entre usuarios y sistemas en la nube.

Las claves de encriptación deben ser almacenadas en ubicaciones seguras y protegidas y debe estar limitado el acceso a las mismas solo a usuarios autorizados y aplicaciones que las necesiten.

4.2. Copias de seguridad y pruebas de recuperación

Se deben realizar copias de seguridad regulares de los datos almacenados en la nube, de acuerdo con la criticidad de los mismos, almacenándolas en ubicaciones geográficamente

separadas y cumpliento con los lineamientos definidos en la norma de **Resguardo y Recupero de la Información** para garantizar la disponibilidad y la recuperación en caso de fallos.

4.3. Monitoreo y detección de amenazas

Se deben implementar herramientas de monitoreo y detección de amenazas para identificar posibles actividades maliciosas en los servicios de la nube. Las mismas deben estar configuradas para identificar eventos críticos como accesos no autorizados, cambios de configuración y transferencias inusuales de datos.

4.4. Respuesta ante incidentes

Se debe contar un plan detallado de respuesta a incidentes y un equipo responsable de la gestión de los mismos, de acuerdo con los lineamientos definidos en la norma de **Gestión de Incidentes de Seguridad** y las acciones detalladas en el procedimiento de **Gestión de Incidentes de Seguridad.**

4.5. Finalización de Servicios

Antes de finalizar un servicio de nube, se debe asegurar la eliminación segura de los datos y recursos asociados, siguiendo los procedimientos de cierre recomendados por el proveedor de servicios de nube.

5. Referencias

5.1. Normativa Relacionada

Categoría	Título	Código
Norma	Gestión de Cuentas de Usuarios	NO-SI-02
Norma	Gestión de Contraseñas	NO-SI-03
Norma	Resguardo y Recupero de la Información	NO-SI-15
Norma	Gestión de Incidentes de Seguridad	NO-SI-10
Procedimiento	Gestión de Incidentes de Seguridad	PR-SI-17

5.2. Definiciones

Término	Descripción
Seguridad	Es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o errores y acciones ilícitas o malintencionadas que comprometan la confidencialidad, integridad y disponibilidad (CIA) de los datos almacenados o transmitidos y de los servicios que dichas redes o sistemas ofrecen o hacen accesibles.

Entorno Cloud	Un entorno cloud o de nube, es un espacio virtual que permite acceder a recursos de computación bajo demanda a través de internet. Esto elimina la necesidad de invertir en equipos físicos y software, ya que se puede alquilar lo que se necesite.

6. Historial de Versiones

Versión	Fecha	Resumen de Cambios
1.0	18/12/2024	Creación del documento
1.0	03/01/2025	Aprobado por Comité de Dirección.