1 Índice

Contenido

2 Objeto

Establecer los lineamientos necesarios a fin de velar por la confidencialidad, integridad y disponibilidad de los activos informáticos y de información de YPF, gestionando los riesgos asociados, minimizando el impacto frente a la posible materialización de amenazas internas o externas a la organización y terceras partes relacionadas.

3 Consideraciones principales

Esta norma se enfoca en orientar al personal en la implementación de objetivos y directrices, con la finalidad de gestionar la Ciberseguridad en YPF reduciendo los riesgos a los que se encuentran expuestos los activos informáticos a niveles asumibles por la Compañía.

Se establecen lineamientos en cumplimiento con el Marco normativo legal , nacional e internacional, así como estándares reconocidos, para proteger los intereses de la Compañía y sus inversores.

Se encuentra basada en las mejores prácticas de Ciberseguridad y abarca a las Tecnologías de Información (IT) y a las Tecnologías de Operaciones (OT), asegurando tanto la continuidad del negocio como la mejora continua en los procesos.

La norma debe ser divulgada internamente para conocimiento y cumplimiento por parte de todo el personal de la Compañía, enfatizando la importancia de la comunicación efectiva en todos los niveles.

El incumplimiento de la presente,conlleva riesgos legales y disciplinarios, incluyendo sanciones civiles y penales, así como la posible terminación de la relación laboral o contractual.

4 Contenido

Esta norma describe las disposiciones relativas a todos los recursos y sistemas informáticos de la Compañía.

4.1 Organización de Ciberseguridad

4.1.1 Organización interna de Ciberseguridad

Definir la estructura para administrar la Ciberseguridad dentro de la Compañía y establecer un marco para controlar su implementación.

Asegurar la firma del compromiso de confidencialidad por parte de todo el personal y terceros relacionados a la Compañía.

4.1.1.1 Roles y responsabilidades de Ciberseguridad

La Gerencia de Ciberseguridad define los roles y funciones requeridos para la correcta y eficiente administración, gestión, operación, control y monitoreo de los mecanismos implementados y para proteger los activos informáticos e industriales de la Compañía.

4.1.1.2 Segregación de funciones

Las tareas privilegiadas o sensibles deben ser separadas de otras similares, para minimizar el riesgo de abuso de privilegio y aumentar la capacidad de control, respetando el principio de segregación de funciones.

4.1.1.3 Contactos con autoridades y grupos de especial interés

La cadena de comunicación con autoridades es determinada por el impacto de un incidente de ciberseguridad, de acuerdo a la clasificación del mismo. Estos incidentes deben ser notificados inmediatamente al personal involucrado dentro de la organización, y se recomienda mantenerse actualizado sobre las mejores practivas y regulaciones a través de la adhesión y suscripción a foros o grupos de interés especial

4.1.2 Dispositivos móviles y trabajo remoto

Teniendo en cuenta los riesgos asociados con entornos no protegidos, es necesario garantizar la gestión segura de la información al utilizar dispositivos móviles y trabajar de forma remota, aplicando medidas de protección adecuadas para salvaguardar la plataforma tecnológica.

Estas medidas de seguridad deben aplicarse según las políticas, normas y procedimientos de la Compañía, estableciendo mecanismos de monitoreo y control, manteniendo un registro específico de auditoría para estos accesos bajo una revisión regular.

Se debe proteger la información y la infraestructura de la Compañía al usar dispositivos móviles, ya que aumenta el riesgo de incidentes por pérdida, robo o hurto. Por tal motivo se debe concientizar al personal que los utilíce y establecer procedimientos para reportar rápidamente cualquier incidente mitigando así, los riesgos de los sistemas de información.

4.2 Seguridad de los recursos humanos

Todos los empleados, proveedores y contratistas, desde su ingreso hasta la finalización de su relación laboral y/o comercial, son responsables del manejo de la información utilizada en cumplimiento de sus funciones. Esta información es propiedad exclusiva de la Compañía excepto en aquellos casos donde la información contenga datos personales, conforme a la Ley de Protección de Datos Personales 25.326.

Están sujetos a las disposiciones de seguridad establecidas por la Gerencia de Ciberseguridad y deben devolver los activos asignados al finalizar la relación laboral y/o comercial. Durante la misma, deben cumplir con el "Código de Ética y Conducta" y la "Política de Ciberseguridad y Seguridad Corporativa" de la Compañía, mientras que la Gerencia de Ciberseguridad proporciona apoyo en estos aspectos.

4.2.1 Capacitación y Concientización en Ciberseguridad

Todo el personal de la Compañía, incluidos los contratados y terceros cuando sea necesario, deben recibir capacitación periódica sobre ciberseguridad, enfocada en requisitos de seguridad, responsabilidades legales y uso correcto de recursos. Se establece un plan estratégico de concientización en ciberseguridad adaptado a las necesidades del negocio.

4.3 Gestión de Ciber Riesgos

4.3.1 Gestionar los Ciber Riesgos

Establecer una metodología de gestión para la identificar, evaluar y tratar los Ciber Riesgos de las Tecnologías de Información (IT), considerando la exposición de la información a las amenazas y

protegiendo la confidencialidad, integridad y disponibilidad de los activos informáticos. El objetivo es minimizar el nivel de riesgo, de acuerdo con los principales controles y buenas prácticas.

4.3.2 Gestionar los Ciber Riesgos Industriales (OT)

Definir una metodología para Evaluación de Riesgos Cibernéticos (ERC) para analizar y proteger los sistemas industriales frente a ciber amenazas maximizando la disponibilidad y resguardando la confidencialidad e integridad de la información en los Sistemas Industriales y reduciendo los riesgos a los niveles tolerables por YPF S.A.

4.4 Gestión de Activos

Los activos deben ser gestionados y protegidos de manera efectiva según su criticidad para el negocio, teniendo en cuenta sus funciones y las normativas aplicables.

4.4.1 Propiedad sobre los Activos de Información

Todo activo informático debe tener designado un propietario que vele por el cumplimiento de sus responsabilidades identificadas, definidas y registradas. Tiene que asegurarse que se realice una correcta clasificación de los activos, inventariados y protegidos, a efectos de evitar su exposición, pérdida o corrupción durante el ciclo de vida establecido.

4.4.2 Clasificación de Activos de Información

Controlar y velar la confidencialidad, integridad y disponibilidad de la información y el dato que se procesa y almacena en los activos informáticos, a través de la correcta identificación y clasificación de la misma, a efectos de evitar su exposición, pérdida o corrupción.

4.4.3 Manipulación de Información en medios removibles:

Se establecen directrices para gestionar los medios según el esquema de clasificación de la Compañía, con el fin de evitar la alteración, transferencia, divulgación, eliminación o destrucción de la información almacenada en estos dispositivos físicos o digitales, utilizados por empleados y terceros.

4.5 Control de Accesos

4.5.1 Administración de Usuarios en Plataformas Tecnológicas

Establecer lineamientos generales para asegurar una adecuada administración de los accesos de los usuarios a los recursos informáticos de YPF y plataformas de Cloud Computing.

4.5.2 Administrar Cuentas de Servicio

Establecer las actividades para la correcta gestión de las Cuentas de Servicios utilizadas en los sistemas de información de YPF, considerando los principales controles y buenas prácticas de la cuenta.

- Resguardo de la contraseña.
- Limitantes de Utilización.
- Nomenclatura.

4.5.3 Gestionar Usuarios de Amplios Privilegios y de Emergencia

Establecer las acciones necesarias para la gestión de usuarios de amplios privilegios y de emergencia implementados en los sistemas de Claves de Ensobrado Electrónico, alcanzando a todos los ambientes (Producción, Desarrollo y Testing).

4.5.4 Seguridad de Contraseñas

Establecer y estandarizar los parámetros de configuración de seguridad de las contraseñas de los sistemas operativos, bases de datos, equipos de comunicación, software de base y aplicaciones.

4.6 Gestión criptográfica

Establecer los controles normativos y técnicos necesarios para gestionar claves criptográficas durante su ciclo de vida, así como los mecanismos de cifrado para proteger los datos en reposo y en tránsito. El objetivo es garantizar la integridad, confidencialidad, no repudio y autenticación de los activosde información de la Compañía.

4.7 Protección física y del entorno:

4.7.1 Áreas Seguras

Los centros de procesamiento de datos deben ubicarse en áreas seguras, protegidos por perímetros definidos y estrictos controles de acceso, conforme a las normas de la Compañía. Los espacios que albergan activos e infraestructura de IT deben ser clasificados y protegidos según su valor y criticidad para garantizar la continuidad del negocio.

El acceso de terceros a estas áreas debe ser controlado por el personal de seguridad y el propietario del activo. Además se deben proteger contra riesgos naturales y amenazas ambientales siguiendo las directrices de la Compañía.

Asimismo, se deben considerar controles de acceso físico, aseguramiento de los centros de datos y protección contra amenazas externas y del entorno.

4.7.2 Equipamiento en CPD

Es fundamental controlar los parámetros ambientales de los CPD para garantizar su correcto funcionamiento y minimizar interrupciones. Los equipos deben tener un mantenimiento periódico, lo que puede requerir trasladarlos fuera de las áreas seguras bajo estrictas medidas de seguridad y considerando la clasificación de la información almacenada en los mismos y los riesgos internos y externos asociados.

4.8 Seguridad en las Operaciones

4.8.1 Separación de Ambientes

Establecer lineamientos que permitan asegurar que los nuevos desarrollos o actualizaciones de software se implementen en un entorno controlado y con una adecuada separación de funciones para minimizar riesgos como cambios no autorizados, errores de desarrollo, implementaciones no probadas, actualizaciones accidentales e interrupciones en la operatoria, entre otros.

4.8.2 Seguridad Antimalware

Establecer requerimientos de antimalware para todos los equipos de clientes y servidores conectados a los sistemas informáticos o redes de la Compañía para prevenir y detectar intrusiones maliciosas y evitar su propagación.

4.8.3 Revisión de Logs

Se deben monitorear los sistemas y componentes de red, a fin de registrar todas las actividades que los usuarios realizan tales como, excepciones, fallos y eventos de seguridad de la información..

4.8.4 Escaneo de Activos Tecnológicos

Establecer los lineamientos generales para ejecutar las actividades de escaneo de vulnerabilidades sobre de activos tecnológicos de la Compañía y de terceros.

4.8.5 Gestión de Vulnerabilidades

Establecer procesos para identificar, analizar, remediar y validar de forma proactiva las vulnerabilidades para mantener los niveles de seguridad de la Compañía.

4.8.6 Gestión de Cambios

Aplicar controles estrictos durante la implementación de cambios en los sistemas de información para reducir riesgos, asegurando el cumplimiento de procedimientos formales y la segregación de funciones.

4.9 Seguridad en Comunicaciones

4.9.1 Seguridad en Comunicaciones internas y externas

Establecer pautas generales para asegurar una adecuada protección de la información en los procesos de transmisión de datos en las redes internas y externas de los sistemas informáticos, considerando los principales controles y buenas prácticas.

4.10 Adquisición, desarrollo y mantenimiento de los sistemas de información

4.10.1 Seguridad para la Adquisición o Desarrollo de Software

Establecer las pautas de seguridad y controles a efectuarse al momento de adquirir o desarrollar software, con el objetivo de reducir a un nivel aceptable los riesgos internos y externos de accesos no autorizados y pérdidas de datos.

4.11 Gestión de incidentes de Ciberseguridad

La Gerencia de Ciberseguridad de la Compañía establece responsabilidades y procedimientos para la respuesta y gestión de incidentes de seguridad de la información, así como mecanismos proactivos para identificar brechas de seguridad, elaborar planes de recuperación y mejorar la resiliencia organizacional. Los incidentes son documentados y resguardados para cumplir con requerimientos legales y posibles investigaciones.

Asimismo, se definen umbrales de criticidad para la respuesta a incidentes, y se gestiona el ciberfraude según su impacto económico y reputacional de la Compañía.

4.11.1 Monitoreo de Eventos de Seguridad

Establecer los lineamientos para realizar el monitoreo de los accesos a recursos y eventos críticos a fin de identificar y dar seguimiento sobre posibles incidentes de seguridad con el objetivo de mitigar riesgos de accesos no autorizados, pérdidas y daños a la información.

4.12 Seguridad en plataformas y aplicaciones

4.12.1 Seguridad en Base de Datos

Establecer pautas de seguridad para configurar bases de datos, limitando los privilegios de usuarios administrativos. Se destaca la designación de roles específicos, procedimientos de instalación, gestión de cuentas y permisos, auditoría de eventos, limitaciones, resguardos y actualizaciones.

4.12.2 Seguridad en Aplicaciones

Establecer lineamientos para garantizar la confidencialidad, integridad y disponibilidad de los sistemas de información, en cumplimiento con políticas y legislaciones externas e internas.

Se destacan controles como asignación de propietarios, separación de ambientes, restricciones de infraestructura, ambientes diseño seguro, acceso mínimo a recursos, plataforma cloud, requerimientos de seguridad y registro/monitoreo continuo.

4.12.3 Seguridad en Sistemas Operativos

Establecer pautas de seguridad para configurar sistemas operativos en servidores, dispositivos finales y máquinas virtuales. Se consideran controles como acceso remoto, administración de cuentas, auditoría, registro de eventos, configuración de red, protección contra amenazas, resguardos y actualizaciones, así como la gestión de obsolescencia, entre otros.

4.12.4 Relación con proveedores

Asegurar la protección de los activos a los que acceden los proveedores asociados a la Compañía, manteniendo un nivel acordado de Seguridad de la Información y de prestación de servicio conforme a los acuerdos establecidos.
Los responsables de los contratos con proveedores deben asegurar que se definan y acuerden los niveles de seguridad. Los mecanismos a implementar incluyen seguridad de la información con proveedores, tratamiento de seguridad en acuerdos de servicio, requisitos de tratamiento de riesgo, gestión de entrega y seguimiento de servicios, así como gestión de cambios en los servicios prestados.

4.13 Seguridad de la información en la Gestión de Continuidad del Negocio

Se deben implementar mecanismos y estrategias para desarrollar, evaluar y activar planes de contingencia, garantizando el restablecimiento de servicios críticos del negocio. Los propietarios de los activos deben elaborar el plan de contingencia y asegurar que el personal conozca su contenido para mantener la continuidad del negocio. Los mecanismos incluyen planificación de la continuidad, documentación e implementación de procesos, procedimientos y controles, revisión y valoración de la continuidad, así como la implementación de redundancia para garantizar la disponibilidad.

4.14 Cumplimiento

4.14.1 Cumplimiento o Conformidad Legal

Establecer lineamientos para garantizar el cumplimiento de la legislación vigente en Argentina especialmente la Ley N° 25.326 de Protección de Datos Personales y su normativa complementaria, aplicables a las obligaciones contraídas por YPF y bajo el marco normativo de la Compañía sobre los activos de información y sistemas informáticos.

Asimismo, establecer directrices para planificar actividades de auditoría que verifiquen los sistemas operativos y minimicen las interrupciones en los procesos comerciales.

4.14.2 Seguridad en Firma Digital

Establecer los lineamientos de seguridad sobre la utilización e implementación de la Firma Digital, con el fin de garantizar la seguridad de los documentos y actos firmados, considerando los principales controles y buenas prácticas.

4.14.3 Seguridad de Datos Personales

Establecer lineamientos para las medidas de seguridad sobre los activos de la información que contengan datos de carácter personal, a fin de asegurar su adecuada protección, conforme a lo establecido por la Ley 25.326 y sus reglamentaciones, considerando los principales controles y buenas prácticas.

4.15 Seguridad en Sistemas Industriales (OT)

4.15.1 Norma General de Ciberseguridad Industrial

Establecer los lineamientos necesarios a fin de asegurar la disponibilidad de los Sistemas Industriales y proteger la disponibilidad, confidencialidad e integridad de los datos procesados y/o almacenados, adoptando medidas de prevención y control.

4.16 Seguridad Cloud

La Compañía establece criterios de seguridad y responsabilidad para la gestión de servicios en la nube, tanto para entornos IT como OT, en colaboración con proveedores y terceros. Se consideran los estándares de la industria y la legislación aplicable para proteger los intereses de la Compañía.

Los aspectos de seguridad que se consideran incluyen recuperación de datos, protección contra robo de datos, prevención de errores humanos, y reducción del impacto de posibles brechas de seguridad. Se diferencian los conceptos de las normativas (IaaS, PaaS o SaaS) y se busca minimizar el impacto de posibles riesgos en los sistemas de información e industriales (OT)