NubeFacT®

Política de Seguridad de la Información

VERSIÓN: V4.0

PUBLICO

OFICIAL

PARA: NUBEFACT

HISTORIAL DE VERSIONES

VERSIÓN	DESCRIPCIÓN	REALIZADO POR	FECHA
V4.0	Reformulación de las 8 políticas, por otras de fácil recordación Se actualizan la versión de los documentos relacionados.	DANTE RICARDO PFEIFFER PALOMINO	2023-07-14
V2.0	vs 3.1. del 06/10/2022 Se actualizan el punto 5.1.1.2 de acuerdo a obj.seg. Actualizar 5.1.1.8 agregando Log de incidencias Se especifican responsables en el punto 5.1.1.9.	DANTE RICARDO PFEIFFER PALOMINO	2022-10-10
V1.0	Versión 3 de la documentación originaria Se incluye definición, objetivos y roles Se precisan las políticas de seguridad difundidas en resumen	DANTE RICARDO PFEIFFER PALOMINO	2022-05-05

Tabla de contenido

Política de Seguridad de la Información

1.Objetivo

El propósito de las Políticas de Seguridad es establecer principios, reglas y lineamientos básicos para la gestión de la seguridad de información en los procesos de entrega de servicios de comprobación informática del cumplimiento de las condiciones de emisión y recepción de los comprobantes electrónicos emitidos, revisados y validados a través de los sistemas de la Empresa.

2. Alcance y Usuarios

Esta Política se aplica a todo el Sistema de gestión de seguridad de la información, según se define en el documento del Alcance del SGSI.

Los usuarios de este documento son todos los empleados de la Empresa, como también terceros externos a la organización, así como el público en general.

3. Documentos de Referencia

- Norma ISO/IEC 27001.
- Lista de obligaciones legales, normativas y contractuales.
- Declaración de Aplicabilidad.
- Documento sobre el alcance del SGSI.
- NF-MAN-001-003 Objetivos de Seguridad
- NF-MAN-001-005 Manual de organización y funciones.
- NF-POL-001-004 Resumen Seguridad de la Información
- NF-POL-001-006 Organización de la seguridad de la información

4. Definiciones sobre seguridad de la Información.

Activo: Cualquier cosa que tiene valor para la empresa.

Activo de información: todo aquello que es o contiene información, son los datos y el conocimiento de las personas, y que tiene valor para la empresa.

Aplicaciones: Es todo el software que se utiliza para la gestión de la información.

Acuerdo de Confidencialidad: documento que los gerentes y empleados de la Empresa o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la empresa, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso.

Alcance: Ámbito de la organización que queda sometido al SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.

Alerta: Una notificación formal indicando que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

Amenaza: Según [ISO/IEC 13335-1:2005]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Auditoría: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Cifrado: es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

Confidencialidad: acceso a la información por parte únicamente de quienes estén autorizados.

Control: toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Criptografía: disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

Datos: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la Empresa.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.

Gestión de claves: Controles referidos a la gestión de claves criptográficas.

Personal: Son las personas que trabajan en la empresa, incluye el personal contratado, subcontratado, usuarios internos, en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la Empresa.

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002]: intención y dirección general expresada formalmente por la Dirección.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2009]: combinación de la probabilidad de un evento y sus consecuencias.

Riesgo Residual: Según [ISO/IEC Guía 73:2009] El riesgo que permanece tras el tratamiento del riesgo.

Segregación de tareas: Separar tareas sensibles entre distintos colaboradores o contratistas para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Servicios: Son los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a clientes y usuarios.

SGSI Sistema de Gestión de la Seguridad de la Información: Según [ISO/IEC 27001: 20013]: la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Tecnología: Son todos los equipos utilizados para gestionar la información y las comunicaciones.

Usuario Externo: Persona que hace uso de las aplicaciones de la Empresa en la web que no son trabajadores de la Empresa.

Usuario interno: Trabajador o colaborador de la Empresa que tienen responsabilidad en una determinada área de la empresa, la que puede ser Sistemas, Soporte, Ventas, Finanzas, etc.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

5. Políticas de Seguridad

5.1. Lineamientos de gestión para la seguridad de la información

5.1.1. Políticas para la seguridad de la información

5.1.1.1. Definición

Conjunto de medidas preventivas y reactivas que hace uso la Empresa para resguardar y proteger su información evitando se afecte su confidencialidad, integridad, disponibilidad y auditabilidad.

5.1.1.2. Objetivos

Los objetivos de seguridad de información, que la Empresa persigue con el establecimiento, implementación, mantenimiento y mejora continua del SGSI, son:

- El personal involucrado en el alcance del SGSI debe estar capacitado y sensibilizado en aspectos de seguridad de información.
- Conservar, salvaguardar y proteger los activos de información producidos por los procesos de la Empresa.
- Gestionar adecuadamente los roles y reglas de acceso en función de las necesidades de la Empresa.
- Gestionar adecuadamente los riesgos que constantemente debe hacer frente la Empresa en sus operaciones diarias.
- Realizar planificadamente una auditoría interna y externa al año.

Los recursos y planes para alcanzar estos objetivos se detallan en el manual:

NF-MAN-001-003 Objetivos de Seguridad

5.1.1.3. Roles y responsabilidades

- Rol: Comité de Seguridad de la Información
- Rol: Oficial de Seguridad de la Información
- Cargo: Todos los Colaboradores
- Área: Recursos Humanos
- Área: Sistemas

En la política NF-POL-001-006 Organización de la seguridad de la información y en el NF-MAN-001-005 Manual de Organización y Funciones se detallan las responsabilidades.

Es el Comité de Seguridad del SGSI de la Empresa el que tiene la responsabilidad de mantener el SGSI y hacer cumplir las políticas de seguridad de la información, con ese fin se han asignado los roles siguientes:

- Alta Dirección.
- Oficial de Seguridad.
- Responsables de los controles del SGSI
- Responsables del monitoreo del SGSI
- Propietarios de la información.

En el Manual del Equipo Implementador del SGSI se detallan las responsabilidades del Comité de Seguridad:

NF-MAN-001-004-Manual Equipo Implementador SGSI

5.1.1.4. Políticas (NF-POL-001-004 Resumen Seguridad de la Información):

- **Asegurar la Confidencialidad, integridad y disponibilidad** de la información.
- Leer y dar cumplimiento a los distintos documentos proporcionados por la Empresa y confirmar su recepción.
- Actualizar y mejorar constantemente el Sistema de Gestión de Seguridad de la Información (SGSI).
- Atender de inmediato cualquier violación de seguridad de la información detectada en la Empresa.
- Realizar y promover evaluaciones, mantenimientos y pruebas periódicas.
- Gestionar los riesgos de Seguridad de la Información.

- Participar en todas las capacitaciones de Seguridad de la Información
- Cumplir con responsabilidad y compromiso las políticas de seguridad de la información y protección de los activos que me asigne la empresa.

5.1.1.5. Asegurar la Confidencialidad, integridad y disponibilidad de la información

Los niveles de clasificación de la información que se ha establecido son: USO INTERNO, PÚBLICO y CONFIDENCIAL.

Debemos tener personal asignado para el monitoreo de nuestras aplicaciones con el fin de garantizar la disponibilidad de nuestros recursos tecnológicos.

Ningún usuario interno debe, ni puede modificar registros de los clientes, solo a solicitud escrita del cliente y autorizado por el Jefe de Sistemas pueden eliminar e incluso ingresar un registro nuevo para ellos. Por lo tanto los registros que han recibido respuesta de los servidores de SUNAT se mantendrán íntegros desde sus inicios.

5.1.1.6. Leer y dar cumplimiento a los distintos documentos proporcionados por la Empresa y confirmar su recepción.

Todo el personal debe revisar y poner en práctica las distintas políticas de seguridad, procedimientos y documentos que recibe por correo electrónico o por otro medio cada vez que son actualizadas.

En ellas se detallan, entre otras, las políticas:

a. Control de accesos (ver NF-POL-001-009).
b. clasificación de la información (ver cap. 4.2 de NF-POL-001-008 Gestión de Activos).
c. seguridad física (Ver NF-POL-001-011).
d. temas orientados al usuario interno, tales como:
    - uso aceptable de activos (ver cap. 4.1.3 de NF-CLA-001-008 Gestión de Activos)
    - escritorio y pantalla limpios (ver cap. 4.2.9 de NF-CLA-001-011 Seguridad física)
    - transferencia de información (ver cap. 4.2.1 de LN-CLA-013 Seguridad en las comunicaciones).
    - dispositivos móviles y teletrabajo (ver cap. 4.2 de NF-CLA-001-006 Organización de la seguridad de la información)
    - restricciones a las instalaciones de software (ver 4.6.2 de LN-CLA-012 Seguridad en las operaciones).
e. respaldo (ver cap. 4.3 de LN-CLA-012 Seguridad en las operaciones).
f. transferencia de información (Ver cap. 4.2 de LN-CLA-013 Seguridad en las comunicaciones).
g. protección contra software malicioso (ver cap. 4.2 de LN-CLA-012 Seguridad en las operaciones).
h. gestión de vulnerabilidades técnicas (ver cap 4.6.1 de LN-CLA-012 Seguridad en las operaciones).
i. controles criptográficos (NF-CLA-001-010).
j. seguridad de las comunicaciones (LN-CLA-013).
k. privacidad y protección de datos personales (ver Cap. 4.1.4 de NF-CLA-001-018 Cumplimiento).
l. relaciones con los proveedores (ver LN-CLA-015).

5.1.1.7. Actualizar y mejorar constantemente el Sistema de Gestión de Seguridad de la Información (SGSI).

La Gerencia debe diseñar, programar y realizar los programas de auditoría del sistema de gestión de seguridad de la información.

La Empresa deberá mantener un inventario o registro actualizado de sus activos de información, bajo la responsabilidad de cada propietario de información y centralizado por la Jefatura de Sistemas.

La documentación actualizada es distribuida al personal previa autorización del Comité de Seguridad.

5.1.1.8. Atender de inmediato cualquier violación de seguridad de la información detectada en la Empresa.

Todo trabajador o usuario interno deberá informar al Jefe Inmediato de cualquier violación de las Políticas de Seguridad o uso indebido que tenga conocimiento, así como las medidas a tomar de acuerdo al procedimiento LN-PRO-001-003 Gestión de incidentes de seguridad de la información.

El personal de sistemas encargado del monitoreo debe revisar los activos críticos de acuerdo al procedimiento NF-PRO-001-030 Monitoreo de equipos remotos, LN-PRO-010 Procedimiento para revisar equipos del personal, entre otros.

5.1.1.9. Realizar y promover evaluaciones, mantenimientos y pruebas periódicas.

El Jefe de Sistemas en coordinación con el Oficial de Seguridad deberán definir o indicar la frecuencia de respaldo y los requerimientos de seguridad de la información (codificación).

El Oficial de Seguridad es el responsable de constatar los respaldos periódicos.

Para ello el área de sistemas debe tomar en cuenta el Procedimiento NF-PRO-001-021 de respaldo de la información y NF-PRO-001-036 Procedimiento de recuperación del sistema.

5.1.1.10. Gestionar los riesgos de Seguridad de la Información.

El Comité de Seguridad del SGSI de la Empresa se reúne periódicamente para detectar los riesgos de seguridad tomando en cuenta la Metodología NF-MET-001-001 de gestión de riesgos de seguridad de la información para la elaboración y actualización del Inventario de activos, evaluación de riesgos, tratamiento del riesgo y declaración de aplicabilidad.

5.1.1.11. Participar en todas las capacitaciones de Seguridad de la Información.

El Oficial de Seguridad periódicamente y de acuerdo al NF-001-001 Plan de concientización y capacitación realizará talleres con las distintas áreas de la Empresa.

Todo el personal debe interesarse y participar de estas capacitaciones y evaluaciones.

5.1.1.12. Cumplir con responsabilidad y compromiso las políticas de seguridad de la información y protección de los activos que me asigne la Empresa.

Los jefes de área deben asegurarse que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad, se realicen correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información de la Empresa.

El Comité de Seguridad del SGSI de la Empresa debe identificar los riesgos a los que está expuesta la información de las distintas áreas, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.

Se debe asegurar que los **Jefes de Oficinas**, **terceros, trabajadores y colaboradores de la Empresa,** entiendan sus responsabilidades en relación con las políticas de seguridad de la información de la Empresa y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de la información (NF-MAN-001-005).

Los usuarios internos deberán utilizar únicamente los programas y equipos autorizados por la Jefatura de Sistemas.

La Gerencia o Jefes de áreas deberán proporcionar al usuario interno los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad de la Empresa.

5.1.2. Revisión de las políticas de seguridad de la información

El encargado de velar por el cumplimiento de las políticas de seguridad de la información dentro de la Empresa es el Oficial de Seguridad de la Información (CISO), quien conjuntamente con el Comité de seguridad de la Información de la Empresa han establecido que las revisiones de las políticas de seguridad de la información se realicen en intervalos de 12 meses (anual).

Se establecieron estos intervalos por el hecho de ser el tiempo suficiente para encontrar patrones que requieran algún tipo de ajuste.

Los patrones que requieran ajustes son ocasionados por las siguientes causas:

- Cambios externos en la Empresa.
- Cambios en las políticas de la SUNAT.
- Cambios internos dentro de la Empresa.
- Incidentes recurrentes, graves que afecten a la Empresa.