




Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 1 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

Contenido


Contenido.....	1
1. Cláusula: Introducción.....	7
1.1. Seguridad de la información	7
1.2. Objetivos de seguridad de la información.....	8
1.3. Términos y definiciones.....	8
2. Cláusula: Alcance de la Política de Seguridad de la Información.....	10
3. Cláusula: Estructura de la política	10
3.1. Cláusulas.....	11
3.2. Categorías de control	11
4. Cláusula: Evaluación y tratamiento de Riesgos	11
4.1. Evaluación de los Riesgos de Seguridad.....	12
4.2. Tratamiento de los Riesgos de Seguridad	13
5. Cláusula: Política de Seguridad de la Información.....	14
5.1. Categoría: Orientación de la Dirección para la Seguridad de la Información .14	
5.1.1. Políticas para la Seguridad de la Información	14
5.1.2. Revisión de la política de seguridad de la información.....	15
6. Cláusula: Organización de Seguridad de la Información.....	16
6.1. Categoría: Organización interna.....	16
6.1.1. Roles y responsabilidades de la seguridad de la información	16
6.1.2. Segregación de funciones.....	20
6.1.3. Contacto con las autoridades	21
6.1.4. Contacto con grupos de interés especial.....	21
6.1.5. Seguridad de la información en la gestión de proyectos.....	21
6.2. Categoría: Dispositivos móviles y acceso remoto	22
6.2.1. Política de dispositivos móviles	22
6.2.2. Acceso Remoto	23
7. Cláusula: Seguridad de los Recursos Humanos	25
7.1. Categoría: Antes del empleo	25
7.1.1. Términos y condiciones de empleo	25
7.2. Categoría: Durante el empleo.....	26

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 2 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		


7.2.1.	Responsabilidad de la Gerencia.....	26
7.2.2.	Concientización, formación y capacitación en seguridad de la información.....	27
7.2.3.	Proceso disciplinario.....	27
7.3.	Categoría: Desvinculación o cambio de puesto.....	28
7.3.1.	Responsabilidades en la desvinculación o cambio de puesto.....	28
8.	Cláusula: Gestión de Activos.....	29
8.1.	Categoría: Responsabilidad por los Activos.....	29
8.1.1.	Inventario de activos.....	29
8.1.2.	Responsabilidad de los Activos.....	30
8.1.3.	Uso aceptable de los activos.....	30
8.1.4.	Retorno de los activos.....	31
8.2.	Categoría: Clasificación de la información.....	31
8.2.1.	Clasificación de la información.....	31
8.2.2.	Rotulado de la información.....	32
8.2.3.	Manipulación de los activos.....	33
8.3.	Categoría: Manipulación de los medios.....	33
8.3.1.	Gestión de medios removibles.....	33
8.3.2.	Disposición final de medios.....	34
8.3.3.	Traslado de medios físicos.....	35
9.	Cláusula: Control de Accesos.....	36
9.1.	Categoría: Requisitos de la gestión para el control de accesos.....	37
9.1.1.	Política de control de accesos.....	37
9.1.2.	Acceso a las redes y a los servicios de red.....	37
9.2.	Categoría: Gestión de Accesos de Usuario.....	38
9.2.1.	Alta y baja de registros de usuario.....	38
9.2.2.	Asignación de accesos del usuario.....	39
9.2.3.	Gestión de los derechos de acceso privilegiado.....	40
9.2.4.	Gestión de la información secreta para la autenticación del usuario.....	40
9.2.5.	Revisión de los derechos de acceso del usuario.....	41
9.2.6.	Remoción o ajuste de los derechos de acceso.....	42
9.3.	Categoría: Responsabilidades del usuario.....	42
9.3.1.	Uso de la información secreta para la autenticación.....	43

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 3 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		


9.4.	Categoría: Control de acceso a los sistemas y a las aplicaciones.....	44
9.4.1.	Restricción de acceso a la información.....	44
9.4.2.	Procedimientos seguros de inicio de sesión.....	44
9.4.3.	Sistema de gestión de contraseñas	45
9.4.4.	Uso de herramientas con privilegios	46
9.4.5.	Control de acceso al código fuente de los programas.....	46
10.	Cláusula: Criptografía.....	47
10.1.	Categoría: Criptografía	48
10.1.1.	Política de uso de controles criptográficos	48
10.1.2.	Gestión de Claves.....	49
11.	Cláusula: Protección Física y del Entorno.....	50
11.1.	Categoría: Áreas seguras	51
11.1.1.	Perímetro de seguridad física	51
11.1.2.	Controles de ingreso físico.....	52
11.1.3.	Aseguramiento de oficinas, recintos, instalaciones	53
11.1.4.	Protección contra amenazas externas y del entorno.....	54
11.1.5.	Trabajo en áreas seguras.....	54
11.1.6.	Áreas de carga y descarga	55
11.2.	Categoría: Equipamiento.....	55
11.2.1.	Ubicación y protección del equipamiento.....	56
11.2.2.	Elementos de soporte	56
11.2.3.	Seguridad del cableado.....	58
11.2.4.	Mantenimiento del equipamiento	58
11.2.5.	Retiro de activos.....	59
11.2.6.	Seguridad del equipamiento y los activos fuera de la organización.....	59
11.2.7.	Disposición final segura o reutilización del equipamiento	60
11.2.8.	Equipamiento desatendido de usuario	60
11.2.9.	Política de escritorio y de pantalla limpios	61
12.	Cláusula: Seguridad de las Operaciones	62
12.1.	Categoría: Procedimientos y responsabilidades operativos	62
12.1.1.	Procedimientos operativos documentados	62
12.1.2.	Gestión del cambio	63

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 4 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		


12.1.3.	Gestión de la capacidad	64
12.1.4.	Separación de los entornos de desarrollo, pruebas y producción.....	64
12.2.	Categoría: Protección contra código malicioso	65
12.2.1.	Controles contra código malicioso.....	65
12.3.	Categoría: Resguardo	66
12.3.1.	Resguardo de la información	67
12.4.	Categoría: Registro y seguimiento	68
12.4.1.	Registro de eventos.....	68
12.4.2.	Protección de la información de los registros.....	68
12.4.3.	Registro de administradores y operadores.....	69
12.4.4.	Sincronización de los relojes.....	69
12.5.	Categoría: Control del software de producción	70
12.5.1.	Instalación del software en los sistemas de producción.....	70
12.6.	Categoría: Gestión de las vulnerabilidades técnicas	71
12.6.1.	Control de las vulnerabilidades técnicas.....	71
12.6.2.	Restricciones a la instalación de software	72
12.7.	Categoría: Consideraciones para las auditorías de sistemas de información 73	
12.7.1.	Controles de la auditoría de sistemas de información.....	73
13.	Cláusula: Seguridad de las Comunicaciones.....	74
13.1.	Categoría: Gestión de la seguridad de la red.....	74
13.1.1.	Controles de red.....	74
13.1.2.	Seguridad de los servicios de red.....	75
13.1.3.	Segregación de redes.....	75
13.2.	Categoría: Transferencia de información.....	76
13.2.1.	Políticas y procedimientos de transferencia de información	76
13.2.2.	Acuerdos de transferencia de información	78
13.2.3.	Mensajería electrónica.....	79
13.2.4.	Acuerdos de confidencialidad	79
14.	Cláusula: Adquisición, Desarrollo y Mantenimiento de los Sistemas	80
14.1.	Categoría: Requisitos de seguridad de los sistemas de información.....	81
14.1.1.	Análisis y especificación de los requisitos de seguridad de la información 81	

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 5 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

14.1.2.	Aseguramiento de los servicios de aplicaciones sobre redes públicas....	82
14.1.3.	Protección de las transacciones de servicios de aplicaciones.....	83
14.2.	Categoría: Seguridad en los procesos de desarrollo y de soporte.....	84
14.2.1.	Política de desarrollo seguro.....	84
14.2.2.	Procedimientos de control de cambios en los sistemas.....	85
14.2.3.	Revisiones técnicas de las aplicaciones luego de cambios en la plataforma de producción.....	86
14.2.4.	Restricciones a los cambios en los paquetes de software.....	86
14.2.5.	Principios de seguridad en el desarrollo de sistemas.....	87
14.2.6.	Entorno seguro de desarrollo.....	88
14.2.7.	Desarrollo provisto por terceras partes.....	88
14.2.8.	Pruebas de seguridad de los sistemas.....	89
14.2.9.	Pruebas de aceptación de los sistemas.....	89
14.3.	Categoría: Datos de prueba.....	90
14.3.1.	Protección de los datos de prueba.....	90
15.	Cláusula: Relaciones con los Proveedores.....	91
15.1.	Categoría: Seguridad de la información en las relaciones con los proveedores.....	91
15.1.1.	Política de seguridad de la información para las relaciones con los proveedores.....	91
15.1.2.	Tratamiento de la Seguridad en los acuerdos con los proveedores.....	92
15.1.3.	Cadena de suministro de las tecnologías de la información y las comunicaciones.....	94
15.2.	Categoría: Gestión de la entrega de servicios prestados por los proveedores	95
15.2.1.	Seguimiento y revisión de los servicios prestados por los proveedores..	95
15.2.2.	Gestión de cambios en los servicios prestados por los proveedores.....	96
16.	Cláusula: Gestión de los Incidentes de Seguridad de la Información.....	97
16.1.	Categoría: Gestión de los incidentes de seguridad de la información y mejoras	97
16.1.1.	Responsabilidades y Procedimientos.....	98
16.1.2.	Presentación de informes sobre los eventos de seguridad de la información.....	99
16.1.3.	Presentación de informes sobre las vulnerabilidades de seguridad de la información.....	99

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 6 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

16.1.4.	Evaluación y decisión sobre los eventos de seguridad de la información	100
16.1.5.	Respuesta a los incidentes de seguridad de la información	100
16.1.6.	Aprendizaje a partir de los incidentes de seguridad de la información ..	101
16.1.7.	Recolección de la evidencia.....	101
17.	Cláusula: Aspectos de Seguridad de la Información en la Gestión de la Continuidad de la gestión	102
17.1.	Categoría: Continuidad de la seguridad de la información	103
17.1.1.	Planificación de la continuidad de la seguridad de la información	103
17.1.2.	Implementación de la continuidad de la seguridad de la información	106
17.1.3.	Verificación, revisión y valoración de la continuidad de la seguridad de la información	107
17.2.	Categoría: Redundancias.....	109
17.2.1.	Disponibilidad de las instalaciones de procesamiento de la información	109
18.	Cláusula: Cumplimiento	109
18.1.	Categoría: Cumplimiento de los requisitos legales y contractuales	109
18.1.1.	Identificación de la legislación y de los requisitos contractuales aplicables.	110
18.1.2.	Derechos de propiedad intelectual	110
18.1.3.	Protección de los registros	111
18.1.4.	Privacidad y protección de la información personal.....	112
18.1.5.	Regulación de controles criptográficos	113
18.2.	Categoría: Revisión de la seguridad de la información	113
18.2.1.	Revisión independiente de la seguridad de la información	113
18.2.2.	Cumplimiento de las políticas y las normas de seguridad.....	114
18.2.3.	Revisión del cumplimiento técnico.....	115

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 7 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

1. Cláusula: Introducción

1.1. Seguridad de la información

La información es un recurso que tiene valor para el Organismo, y por consiguiente debe ser debidamente protegida, teniendo en cuenta especialmente su exposición a un número creciente y una variedad de amenazas y vulnerabilidades.

La información se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma. Puede presentarse de maneras textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro. Cualquiera sea la forma que adquiera la información, o los medios por los cuales se distribuye o almacena, siempre debe estar adecuadamente protegida.


La Seguridad de la Información es la protección de la información de una amplia variedad de amenazas, con el objeto de asegurar la continuidad de la ejecución de las acciones en cabeza del INTI, minimizar los riesgos y maximizar la eficiencia de la organización.

La Seguridad de la Información se logra implementando un conjunto adecuado de controles de seguridad, los cuales incluyen políticas, procesos, procedimientos, funciones del software y del hardware. Estos controles se deben establecer, implementar, supervisar, revisar y mejorar, cuando sea necesario, para garantizar que se alcancen los objetivos específicos de seguridad y del Organismo. Esto debe realizarse en conjunto con el resto de los procesos de gestión.

La identificación de los controles a ser implementados se debe planificar de manera cuidadosa, con atención en los detalles y en armonía con el resto de los sistemas de gestión del Instituto. La gestión de la seguridad de la información requiere como mínimo de la participación de todos los empleados del Organismo, entendiéndose la participación como el conocimiento y el cumplimiento de las normas y procedimientos de seguridad definidos en este contexto.

El desarrollo e implementación de los controles que se desprendan de esta política de seguridad informática deben fortalecer el funcionamiento transversal del organismo, en dialogo y articulación con todas las áreas según sean sus pertinencias, definidas por sus misiones y funciones.

Esta política adhiere al estándar de seguridad IRAM/ISO, tomando como referencia principal la familia de normas ISO 27000, las cláusulas y controles aquí expresados tienen por objetivo marcar un lineamiento de controles a implementar por las áreas del organismo, sin que esto implique modificaciones de estructura y sin afectar los sistemas de gestión existentes, esta política define un sistema de gestión propio de seguridad, del cual se desprenderán políticas, normas, procedimientos y controles para ser considerados por los sistemas de gestión y áreas del organismo con el objetivo de mantener y mejorar la seguridad de la información.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 8 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

1.2. Objetivos de seguridad de la información

- Promover una política pública que enmarque una conducta responsable en materia de seguridad de la información, del organismo, sus agentes y funcionarios.
- Evidenciar el compromiso e interés de quienes componen al instituto en pos del desarrollo de una cultura de ciberseguridad.
- Proteger los recursos de información del Organismo y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de los principios y estándares de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
- Asegurar la implementación de las medidas de seguridad determinadas por el Comité de Gestión de Seguridad de la Información (CGS, en adelante), identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.
- Mantener actualizada la Política de Seguridad de la Información del Organismo, a efectos de asegurar su vigencia y nivel de eficacia.
- Administrar la seguridad de la información dentro del Organismo y establecer un marco gerencial para iniciar y controlar su implementación, así como la distribución de funciones y responsabilidades.
- Garantizar el cumplimiento de la Misión del INTI.

El CGS establece, en la confección y mantenimiento de la presente política, una dirección coincidente con los objetivos del Organismo y demuestra apoyo y compromiso con respecto a la seguridad de la información, promoviendo la mejora continua de los procesos y apoyando otros roles pertinentes de la dirección para que demuestren su liderazgo aplicado a sus áreas de responsabilidad.


La determinación y selección de los objetivos de control a implementar, se fijan en el marco de la selección de controles, a través del análisis de riesgo y de aplicabilidad determinado en un procedimiento formal de análisis y tratamiento de riesgos.

1.3. Términos y definiciones


Seguridad de la Información: entiende la preservación de las siguientes características:

- **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deben considerarse los conceptos de:

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 9 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- **Autenticidad:** busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Auditabilidad:** define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- **Protección a la duplicación:** consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grave una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- **No repudio:** se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
- **Confiabilidad de la Información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- **Activos:** De acuerdo a la ISO 27000 (conjunto de estándares internacionales sobre la Seguridad de la Información), los activos se refieren a cualquier información o elemento relacionado con el tratamiento de dicha información que tengan valor para la organización. Algunos ejemplos de activos son bases de datos, archivos físicos, sistemas de información, cableado y redes, dispositivos de almacenamiento y las mismas personas que manejan datos o conocimiento específico del organismo.
- **Evaluación de Riesgos:** Se entiende por Evaluación de Riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de su procesamiento, la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.
- **Tratamiento de Riesgos:** Proceso de selección e implementación de medidas para modificar el riesgo.
- **Gestión de Riesgos:** Actividades coordinadas para dirigir y controlar una organización en lo que concierne al riesgo.
NOTA. La Gestión de Riesgos usualmente incluye la evaluación de riesgos, el tratamiento de riesgos, la aceptación de riesgos y la comunicación de riesgos.
- **Comité de Gestión de Seguridad de la Información (CGS):** El CGS es un cuerpo integrado por quien ejerce la Presidencia del Instituto y la titularidad de las Direcciones Administrativa, Operativa y de Comercialización y Planificación.
- **Responsable de Seguridad de la Información (RSI):** Es quien cumple la función de supervisar, planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones de cumplimiento de la Política de Seguridad de Información y de asesorar en materia de Seguridad de la Información a los integrantes del Organismo que así lo requieran.
- **Responsable Primario de la Información (RPI):** Son responsables como oficiales de seguridad, de la implementación y del cumplimiento de la Política de Seguridad de la Información dentro de sus áreas de responsabilidad.
- **Incidente de Seguridad:** Un Incidente de Seguridad es un evento adverso en un sistema de información, ya sean computadoras, red de computadoras

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 10 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

u otros medios que contengan información, que puede comprometer o compromete la confidencialidad, integridad y/o disponibilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

- **Riesgo:** Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias o impacto.
- **Amenaza:** Una causa potencial de un incidente no deseado, el cual puede ocasionar daños a un sistema u organización.
- **Vulnerabilidad:** Una debilidad de un activo o grupo de activos que puede ser aprovechada por una amenaza.
- **Control:** Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizacionales, las cuales pueden ser de naturaleza administrativa, técnica, de gestión, o legal. **NOTA.** Control es también utilizado como sinónimo de salvaguarda o de contramedida.

2. Cláusula: Alcance de la Política de Seguridad de la Información

Esta Política se aplica en todo el ámbito del INTI, a sus recursos y a la totalidad de sus procesos, ya sean internos o externos vinculados a la misma, ya sea a través de contratos o acuerdos con terceros y que estén aplicados y relacionados con la información administrada por el Organismo.


Además, la Política de Seguridad de la Información (En adelante PSI) debe ser conocida y cumplida por todo el personal del Organismo, sin distinción de régimen y/o situación de revista, nivel jerárquico, lugar de prestación de servicios, así como también aquellos terceros usuarios (personas humanas, jurídicas, otros organismos) vinculados al INTI en razón del cumplimiento de determinada/s tarea/s específicas.

A tales efectos, la presente PSI deberá ser comunicada a todos los sujetos mencionados en el párrafo anterior, en forma oportuna, clara y detallada.

Se establece como falta el incumplimiento de los lineamientos y disposiciones de esta Política, por parte de los/as agentes y funcionarios/as, en función de lo dispuesto por el régimen sancionatorio establecido en la Ley Marco de Regulación de Empleo Público Nacional N° 25.164, su Decreto Reglamentario N° 1421/02 y sus normas modificatorias y complementarias. Para ello, se establece una graduación en las responsabilidades y sanciones administrativas que se aplicarán de acuerdo con la gravedad de la infracción cometida, sin perjuicio de las acciones legales que pudieran corresponder.

3. Cláusula: Estructura de la política

Esta Política se divide en dos (2) partes, y guarda la siguiente estructura:

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 11 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- Tres (3) cláusulas introductorias, con los términos generales, alcance y el establecimiento de la evaluación y el tratamiento de los riesgos;
- Quince (15) cláusulas que abarcan los diferentes aspectos o dominios de la Seguridad de la Información en concordancia con la IRAM-ISO-IEC 27001:2015 y la IRAM-ISO-IEC 27002. Se presentan de manera sistemática y consistente. Asimismo, en coordinación con las pautas mínimas establecidas por la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN en su Decisión Administrativa N°641/2021.

Cada cláusula contiene un número de categorías o grupo de controles de seguridad principales.

Estos controles servirán de lineamientos para el establecimiento de un marco de criterios institucionales a ser incorporados en la elaboración y actualización de los procesos, armónicamente con las metodologías y pautas definidas en los sistemas de calidad, áreas institucionales dedicadas a la gestión y diseño de procesos, e instancias abocadas a la verificación de eficacia de los controles internos. De tal forma, los criterios que integran la PSI y las definiciones tomadas por él CSI, se incorporan de manera sinérgica dentro de la estructura funcional del organismo, respetando las pertinencias de cada área interviniente.

3.1. Cláusulas

Cada cláusula que define los controles, contiene una o más categorías principales de seguridad.

El orden de las cláusulas no implica su importancia. Dependiendo de las circunstancias, los controles de seguridad o de todas las cláusulas deben ser consideradas.

3.2. Categorías de control

Cada categoría principal de control de seguridad contiene:


- a) un objetivo de control que indica lo que se pretende lograr y
- b) uno o más controles que se pueden aplicar para alcanzar el objetivo de control.

Las descripciones de control se estructuran de la siguiente manera:

Control: define la declaración específica del control, para satisfacer el objetivo de control. Acto seguido se declara la acción a tomar para implementar el control descripto.

4. Cláusula: Evaluación y tratamiento de Riesgos

Toda organización se encuentra expuesto a riesgos en materia de seguridad de la información. No existe la seguridad absoluta, por lo que es necesario conocer cuál es el mapa de riesgos al cual se enfrenta INTI y tomar acciones tendientes a minimizar los posibles efectos negativos de la materialización de dichos riesgos.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 12 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

Es por ello que resulta imprescindible gestionar los riesgos del INTI, como pilar fundamental para la gestión de seguridad.

Objetivo de control

Conocer los riesgos a los que se expone el INTI en materia de seguridad de la información.

Generar información de utilidad para la toma de decisiones en materia de controles de seguridad.

Alcance

La PSI se aplica a toda la información administrada en el Organismo, cualquiera sea el soporte en que se encuentre.

Responsabilidad

El CGS es responsable de que se gestionen los riesgos de seguridad de la información, brindando su apoyo para el desarrollo de dicho proceso y su mantenimiento en el tiempo, sin que esto interfiera y en armonía con las instancias del instituto en materia de evaluación de riesgos.


El RSI junto con los RPI son responsables del desarrollo del proceso de gestión de riesgos de seguridad de la información.

4.1. Evaluación de los Riesgos de Seguridad

El INTI a través del CGS, evaluará sus riesgos, identificándolos, cuantificándolos y priorizándolos en función de los criterios de aceptación de riesgos y de sus objetivos de control relevantes. Los resultados guiarán y determinarán la apropiada acción de la dirección y las prioridades para gestionar los riesgos de seguridad de la información y para la implementación de controles seleccionados para protegerse contra estos riesgos.

Se debe efectuar la evaluación de riesgos periódicamente, para tratar con los cambios en los requerimientos de seguridad y en las situaciones de riesgo, por ejemplo: cambios producidos en activos, amenazas, vulnerabilidades, impactos, valoración de riesgos. Asimismo, se debe efectuar la evaluación cada vez que ocurran cambios significativos. Es necesario que estas evaluaciones de riesgos se lleven a cabo de una manera metódica capaz de producir resultados comparables y reproducibles.

El alcance de una evaluación de riesgos en materia de seguridad de la información, puede incluir a todo el Organismo, una parte, un sistema de información particular, componentes específicos de un sistema, o servicios. Es necesario seguir una metodología de evaluación de riesgos para llevar a cabo el proceso.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 13 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

4.2. Tratamiento de los Riesgos de Seguridad

Antes de considerar el tratamiento de un riesgo, el INTI debe decidir los criterios para determinar si los riesgos pueden, o no, ser aceptados. Los riesgos pueden ser aceptados si, por ejemplo: se evaluó que el riesgo es bajo o que el costo del tratamiento no es económicamente viable para el Organismo. Tales decisiones deben ser tomadas por el CGS y debidamente documentadas.

Para cada uno de los riesgos identificados durante la evaluación de riesgos, se necesita tomar una decisión para su tratamiento. Las posibles opciones para el tratamiento de riesgos incluyen:


- a) Mitigar los riesgos mediante la aplicación de controles apropiados para reducir los riesgos;
- b) Aceptar los riesgos de manera objetiva y consciente, siempre y cuando éstos satisfagan claramente la política y los criterios de aceptación de riesgos del Organismo;
- c) Evitar los riesgos, eliminando las acciones que dan origen a la ocurrencia de éstos;
- d) Transferir los riesgos asociados a otras partes interesadas, por ejemplo: compañías de seguro o proveedoras/es.

Para aquellos riesgos donde la decisión ha sido la mitigación, se buscará reducir los riesgos a un nivel aceptable mediante la implementación de controles, teniendo en cuenta lo siguiente:

- a) Requerimientos y restricciones de legislaciones y regulaciones nacionales e internacionales;
- b) Objetivos organizacionales;
- c) Requerimientos y restricciones operativos;
- d) Costo de implementación y operación en relación directa a los riesgos reducidos, y proporcionales a los requerimientos y restricciones del Organismo;
- e) Equilibrio de las inversiones en la implementación y operación de los controles contra el daño que podría resultar de las fallas de seguridad.

Los controles a implementar pueden ser seleccionados del contenido de las cláusulas de esta política, o se pueden establecer nuevos controles para satisfacer necesidades específicas del Organismo. Es necesario reconocer que algunos controles pueden no ser aplicables a todo sistema de información o a su ambiente, y podrían no ser aplicables en todos los casos.

Se debe recordar que ningún conjunto de controles puede alcanzar la seguridad absoluta. Los controles implementados deben ser evaluados permanentemente para que puedan ser mejorados en eficiencia y efectividad.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 14 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

5. Cláusula: Política de Seguridad de la Información

5.1. Categoría: Orientación de la Dirección para la Seguridad de la Información

Objetivo de control

Proporcionar la orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos de la gestión y las leyes y regulaciones pertinentes.

5.1.1. Políticas para la Seguridad de la Información

Control

Se debe definir un conjunto de políticas para la seguridad de la información, aprobadas por la dirección, publicarlas y comunicarlas a los empleados y a las partes externas pertinentes.

Esta PSI se conforma por una serie de pautas sobre aspectos específicos de la seguridad de la información, que incluyen los siguientes tópicos:

Organización de la Seguridad de la Información: destinada a administrar la seguridad de la información dentro del Organismo y establecer un marco gerencial para controlar su implementación, los criterios básicos y los tipos de clasificación de la misma.


Seguridad de los Recursos Humanos: destinada a reducir los riesgos de error humano, mal desempeño, incumplimiento de los deberes y obligaciones, incurrimento de ilícitos contra el Organismo o uso inadecuado de instalaciones.

Gestión de Activos: destinada a establecer una clasificación de la información completa y actualizada y mantener una adecuada protección de los activos del Organismo.

Control de Acceso: destinada a controlar el acceso lógico de la información.

Criptografía: destinada a establecer los criterios para la gestión, desarrollo e implementación de claves y controles criptográficos para la protección de la información.

Seguridad Física y del Entorno: destinada a impedir accesos no autorizados, daños e interferencias a las sedes e información del Organismo.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 15 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

Seguridad en las Operaciones: dirigida a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.

Seguridad de las Comunicaciones: dirigida a garantizar el funcionamiento correcto y seguro de los medios de Comunicación.

Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información: destinada a garantizar la incorporación de medidas de seguridad en los sistemas de información, ya sea desde su adquisición, su desarrollo e implementación, y durante su mantenimiento en régimen.

Relación con los Proveedores: destinada a gestionar la relación con los proveedores en lo que respecta a los aspectos de seguridad que tienen que ver con el establecimiento y el acuerdo de todos los requisitos de seguridad de la información del Organismo.

Gestión de Incidentes de Seguridad de la Información: destinada a garantizar que los eventos de seguridad de la información se comuniquen de forma tal que se apliquen las acciones correctivas en tiempo y forma.

Aspectos de la Seguridad de la Información en la Gestión de la Continuidad de la Gestión: tiene en cuenta las acciones para contrarrestar las interrupciones de las actividades de procesamiento de la información y proteger los procesos críticos de los impactos de las fallas significativas y/o desastres.

Cumplimiento: destinado a Garantizar que los sistemas informáticos cumplan con la Política, Normas y Procedimientos de Seguridad del Organismo.


5.1.2. Revisión de la política de seguridad de la información

Control

Las políticas de seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar que continúan siendo apropiadas, adecuadas y eficaces.

La política de seguridad de la información debe tener un responsable de las actividades de desarrollo, evaluación y revisión de la política.

La actividad de revisión debe incluir las oportunidades de mejora, en respuesta a los cambios, entre otros: organizacionales, normativos, legales, de terceros, tecnológicos.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 16 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

Las mejoras tenidas en cuenta deben quedar registradas y tener las aprobaciones de los responsables.

El CGS debe revisarla a intervalos planeados y prever el tratamiento de caso de los cambios no planeados, a efectos de mantener actualizada la política.

Asimismo, efectuará toda modificación que sea necesaria en función a posibles cambios que puedan afectar su definición, como ser, cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, etc.

6. Cláusula: Organización de Seguridad de la Información

Generalidades

La presente PSI establece la administración de la seguridad de la información como parte fundamental de los objetivos y actividades del Organismo. Por ello se define formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de la PSI, la coordinación de su implementación y la asignación de funciones y responsabilidades.

Asimismo, se contempla la necesidad de disponer de fuentes con conocimiento y experimentadas para el asesoramiento, cooperación y colaboración en materia de seguridad de la información.

Por otro lado, debe tenerse en cuenta que ciertas actividades del Organismo pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información. En estos casos, se considera que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se deben establecer las medidas adecuadas para la protección de la información.


6.1. Categoría: Organización interna

Objetivo de control

Establecer un marco de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro del Organismo.

6.1.1. Roles y responsabilidades de la seguridad de la información

Control

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 17 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

Se deben definir y asignar todas las responsabilidades relativas a la seguridad de la información.

ROLES

COMITÉ DE GESTIÓN DE SEGURIDAD

La seguridad de la información es una responsabilidad de las máximas autoridades del INTI. Para ello se crea el CGS, integrado por quienes ejercen la Presidencia del Instituto y las Direcciones Administrativa, Operativa y de Comercialización y Planificación.

Funciones:

- Aprobar las iniciativas sobre seguridad de la Información.
- Asegurar el establecimiento de la política y los objetivos de la seguridad de la información y su compatibilidad con la dirección estratégica del Organismo;
- Asegurar la disponibilidad de los recursos necesarios para la gestión de la seguridad de la información;
- Comunicar la importancia de una gestión de la seguridad de la información eficaz;
- Requerir informes y controles necesarios para asegurar el monitoreo y revisión la política, normas y procedimientos;
- Evaluar los desvíos a fin de encaminar las acciones correspondientes cuando corresponda;
- Proponer los cambios normativos que se requieran;

RESPONSABLE DE SEGURIDAD DE LA INFORMACION


Definición:

Quien ejerce la titularidad de la Subgerencia Operativa de Informático y/o el área que la reemplace en el futuro, sea una persona y/o área que tiene la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran.

El INSTITUTO NACIONAL DE TECNOLOGÍA INDUSTRIAL (INTI), en la medida que existen las posibilidades jurídicas y presupuestarias, creará un Departamento de Seguridad de la Informática, cuyo titular ejercerá las funciones asignadas al Responsable de Seguridad de la Información.

Funciones:

- Cumplir funciones relativas a la seguridad de los sistemas de información del Organismo, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la Política de Seguridad de la Información;

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 18 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- Asistir al personal del Organismo en materia de seguridad de la información y coordina la interacción con Organismos especializados. Asimismo, junto con los RPI, analiza el riesgo de los accesos de terceros a la información del Organismo y verifica la aplicación de las medidas de seguridad necesarias para la protección de la misma;
- Coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios;
- Encargarse de coordinar los conocimientos y las experiencias disponibles en el Organismo a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Puede obtener asesoramiento de otros Organismos. Con el objeto de optimizar su gestión, se habilita al RSI el contacto con las Unidades Organizativas de todas las Áreas del Organismo;
- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes;
- Tomar conocimiento y supervisa la investigación y monitoreo de los incidentes relativos a la seguridad;
- Revisar y proponer al CGS para su aprobación la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información;
- Coordinar el proceso de administración de la continuidad de las actividades del Organismo, frente a interrupciones imprevistas;


RESPONSABLE PRIMARIOS DE LA INFORMACION

Definición:

Todo personal con cargo mínimo de jefe de departamento en el INTI, son responsables como oficiales de seguridad, de la implementación y del cumplimiento de la Política de Seguridad de la Información dentro de sus áreas de responsabilidad.

Funciones:

- Informar sobre cualquier cambio que afecte el inventario de activos;
- Clasificar los activos en función a su valor;
- Definir los requisitos de seguridad de los activos;
- Velar por la implementación y el mantenimiento de los controles de seguridad requeridos en los activos;
- Cabe aclarar que, si bien los RPI pueden delegar la administración de sus funciones a personal idóneo a su cargo, conservarán la responsabilidad del cumplimiento de las mismas. La delegación de la administración por parte de los RPI será documentada por los mismos y proporcionada al RSI, mediante una Comunicación Oficial vía el sistema GDE.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 19 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

USUARIOS DE LA INFORMACION

Definición:

Usuarios de la información y de los sistemas utilizados para su procesamiento.

Funciones:

Conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.

RESPONSABILIDADES

El CGS será el responsable de impulsar la implementación de la presente Política.

El RSI tendrá a cargo el mantenimiento y la presentación para la aprobación de la presente Política, ante el CGS, el seguimiento de acuerdo a las incumbencias propias de cada área de las actividades relativas a la seguridad de la información (análisis de riesgos, monitoreo de incidentes, supervisión de la investigación, implementación de controles, administración de la continuidad, impulsión de procesos de concientización, etc.).

Asistirá al personal del Organismo en materia de seguridad de la información y coordinará la interacción con Organismos especializados. Asimismo, junto con los Responsables Primarios de la Información, analizará el riesgo de los accesos de terceros a la información del Organismo y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma.

Los RPI son responsables de:

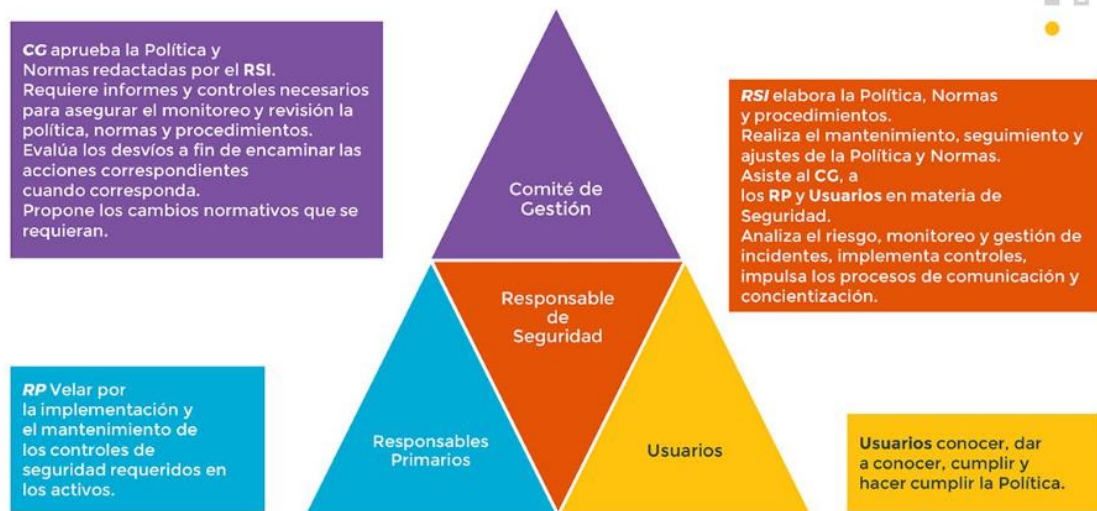
- clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma,
- documentar y mantener actualizada la clasificación efectuada, y
- definir qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

La Unidad de Auditoría Interna, la Unidad de Control de Gestión o en su defecto quien sea propuesto por el CGS será responsable de realizar revisiones independientes sobre la vigencia y el cumplimiento de la presente Política.

Quien ejerza la titularidad de la Gerencia Operativa de Administración y Finanzas cumplirá la función de incluir en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios cuya actividad afecte directa o indirectamente a los activos de información, la obligatoriedad del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas relacionadas.

Quien ejerza la titularidad de la Gerencia Operativa de Administración y Finanzas notificará a los proveedores sobre las modificaciones que se efectúen a la Política de Seguridad de la Información del Organismo.

Estructura organizativa de seguridad




6.1.2. Segregación de funciones.

Control

Se deben segregar las obligaciones y las áreas de responsabilidad incompatibles para reducir las oportunidades de modificación no autorizada o no intencional, o mal uso de los activos del Organismo.

Se debe tener cuidado de que ninguna persona pueda acceder, modificar o usar los activos sin autorización o detección. Se debe separar la ejecución de un evento de su autorización. Al diseñar los controles se debe considerar la posibilidad de complicidad.

En procesos pequeños, entiéndase como proceso pequeño a todos aquellos que son ejecutados por un solo rol, puede encontrarse que la segregación de funciones es difícil de lograr, pero se debe aplicar el principio tanto como sea posible y practicable. Cuando sea difícil segregar, se debe considerar otros controles tales como el monitoreo de actividades, los registros para la auditoría y la supervisión gerencial.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 21 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

6.1.3. Contacto con las autoridades

Control

Se debe mantener los contactos apropiados con las autoridades pertinentes, particularmente con la Dirección Nacional de Ciberseguridad dependiente de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN.

Se deberá tener procedimientos que especifiquen cuándo y a qué autoridades (Policiales, Cuerpo Bomberos, entes reguladores como energía, servicios, entre otros.) contactar para reportar oportunamente los incidentes de seguridad de la información identificados.

6.1.4. Contacto con grupos de interés especial

Control

Se debe mantener los contactos apropiados con grupos de interés especial u otras asociaciones profesionales y foros de especialistas en seguridad.

El RSI será el encargado de coordinar los conocimientos y las experiencias disponibles en el Organismo a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Éste podrá obtener asesoramiento de otros Organismos. Con el objeto de optimizar su gestión, se habilitará al Responsable de Seguridad de la Información el contacto con las Unidades Organizativas de todas las Áreas del Organismo.


Debe considerar ser miembro de grupos de interés especial para:

- a) Adquirir nuevos conocimientos acerca de las mejores prácticas y estar actualizado;
- b) Asegurar que la concientización acerca de la seguridad de la información esté actualizada y completa;
- c) Recibir alertas tempranas, avisos y recomendaciones ante ataques y vulnerabilidades;
- d) Proporcionar vínculos adecuados durante el tratamiento de los incidentes de seguridad de la Información.

6.1.5. Seguridad de la información en la gestión de proyectos

Control

En la gestión de proyectos, se debe considerar la seguridad de la información, independientemente del tipo de proyecto.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 22 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

Se deberá contar con una metodología de gestión de proyectos que especifiquen los siguientes requerimientos:

- a) los objetivos de seguridad de la información se incluyan en los objetivos del proyecto;
- b) se realice una evaluación de riesgos respecto de la seguridad de la información en una etapa temprana del proyecto para identificar los controles necesarios;
- c) la seguridad de la información forme parte de todas las fases de la metodología de proyectos aplicada.

Se deben revisar regularmente las implicancias de la seguridad de la información en todos los proyectos. Se deben definir y asignar las responsabilidades para la seguridad de la información a roles específicos definidos en los métodos de gestión de proyectos.

6.2. Categoría: Dispositivos móviles y acceso remoto

Objetivo de control

Garantizar la seguridad en el acceso remoto y en el uso de dispositivos móviles.

6.2.1. Política de dispositivos móviles

Control

Se debe adoptar una política y las medidas de seguridad adecuadas para gestionar los riesgos ocasionados por el uso de dispositivos móviles.

Dispositivos Móviles


Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información ni la infraestructura del Organismo.

Se debe tener en cuenta en este sentido, cualquier dispositivo móvil y/o removible, incluyendo: Notebooks, Laptop, Teléfonos Celulares y sus tarjetas de memoria, Dispositivos de Almacenamiento removibles, tales como CDs, DVDs, Tapes, y cualquier dispositivo de almacenamiento de conexión USB, Tarjetas de identificación personal (control de acceso), dispositivos criptográficos, cámaras digitales, etc.

Esta lista no es taxativa, ya que deben incluirse todos los dispositivos que pudieran contener información confidencial del Organismo y, por lo tanto, ser pasibles de sufrir un incidente en el que se comprometa la seguridad del mismo.

Se desarrollarán procedimientos adecuados para estos dispositivos, que abarquen los siguientes conceptos:

- a) La protección física necesaria.
- b) El acceso seguro a los dispositivos.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 23 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- c) La utilización segura de los dispositivos en lugares públicos.
- d) El acceso a los sistemas de información y servicios del Organismo a través de dichos dispositivos.
- e) Las técnicas criptográficas a utilizar para la transmisión de información clasificada.
- f) Los mecanismos de resguardo de la información contenida en los dispositivos.
- g) La protección contra software malicioso.

La utilización de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo de pérdida, robo o hurto. En consecuencia, debe entrenarse especialmente al personal que los utilice.

Se deben desarrollar procedimientos sobre los cuidados especiales a observar ante la posesión de dispositivos móviles, que contemplarán las siguientes recomendaciones:

- a) Permanecer siempre cerca del dispositivo.
- b) No dejar desatendidos los equipos.
- c) No llamar la atención acerca de portar un equipo valioso.
- d) No poner identificaciones del Organismo en el dispositivo, salvo los estrictamente necesarios.
- e) La inactivación, el borrado o el bloqueo remotos.
- f) No poner datos de contacto técnico en el dispositivo.
- g) Mantener cifrada la información clasificada.
- h) Por otra parte, se confeccionarán procedimientos que permitan al poseedor del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información del Organismo, los que incluirán:
 - 1) Revocación de las credenciales afectadas.
 - 2) Notificación a grupos de Trabajo donde potencialmente se pudieran haber comprometido recursos.
 - 3) Separación del uso personal del laboral.


6.2.2. Acceso Remoto

Control

Se debe implementar una política y las medidas de seguridad adecuadas para proteger la información que se accede, procesan y almacena desde un acceso remoto.

Acceso Remoto

El acceso remoto utiliza tecnologías de comunicaciones para permitir que el personal realice trabajos en forma remota desde un lugar externo al Organismo.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 24 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

El acceso remoto será autorizado según el procedimiento definido para tal fin, el RSI verificara que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con la política, normas y procedimientos existentes.

Estos casos serán contemplados en situaciones que justifiquen la imposibilidad de otra forma de acceso y la urgencia, tales como horarios del Organismo, solicitud de las autoridades, etc.

Para ello, se deben establecer procedimientos para el acceso remoto, que consideren los siguientes aspectos:


- a) Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos del Organismo, la sensibilidad de la información a la que se accederá y que pasará a través del vínculo de comunicación y la sensibilidad del sistema interno.
- b) La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, por ejemplo, familia y amigos.
- c) Evitar la instalación / desinstalación de software no autorizado por el Organismo.

Los controles y disposiciones comprenden:

- a) Definir el tipo de acceso, la clasificación de la información que se puede almacenar en el equipo remoto desde el cual se accede a la red del Organismo y los sistemas internos y servicio a los cuales el trabajador remoto está autorizado a acceder.
- b) Proveer de un adecuado equipo de comunicación, con inclusión de métodos para asegurar el acceso remoto.
- c) Definir reglas y orientación respecto del acceso de terceros al equipamiento e información.
- d) Proveer el hardware y el soporte y mantenimiento del software de ser necesario.
- e) Definir los procedimientos de back up y de continuidad de las operaciones.
- f) Efectuar auditoría y monitoreo de la seguridad.
- g) Realizar la anulación de las autorizaciones, derechos de acceso y devolución del equipo cuando finalicen las actividades remotas.
- h) Asegurar el reintegro del equipamiento en las mismas condiciones en que fue entregado, en el caso en que cese la necesidad de trabajar en forma remota.

Se implementarán procesos de auditoría específicos para los casos de accesos remotos, que serán revisados regularmente.

Se llevará un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 25 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

7. Cláusula: Seguridad de los Recursos Humanos

Responsabilidad

Quien ejerza la titularidad de la Gerencia Operativa de Recursos Humanos y/o el área que en el futuro la reemplace incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de trabajo a los empleados del Organismo. Además, tendrá la responsabilidad de informar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y del Compromiso de Confidencialidad.

Quien ejerza la titularidad de la Gerencia Operativa de Recursos Humanos junto con el RPI, coordinarán las tareas de capacitación de usuarios respecto de la presente Política y el tratamiento de incidentes de seguridad que requieran de su intervención.

El titular de la Gerencia Operativa de Asuntos Legales junto con quien ejerza la titularidad de la Gerencia Operativa de Recursos Humanos gestionará y confeccionará los compromisos de confidencialidad con los empleados, personal contratado y usuarios de terceras partes que desarrollen funciones en el Organismo y participaran en el tratamiento de las sanciones a ser aplicadas por incumplimiento de la política.

Todo el personal del Organismo, contratistas y usuarios de terceras partes serán responsables del cumplimiento de la Política de Seguridad de la Información del INTI.

7.1. Categoría: Antes del empleo

Objetivo de control

Asegurar que los empleados y personal contratado entiendan sus responsabilidades y sean idóneos para los roles para los cuales se los considera.


7.1.1. Términos y condiciones de empleo

Control

Los contratos laborales con empleados y personal contratado deben establecer sus responsabilidades y las del Organismo para con la seguridad de la información.

Como parte de sus términos y condiciones iniciales de empleo, los empleados, cualquiera sea su situación de revista, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información del Organismo. La copia firmada del Compromiso debe ser retenida en forma segura por la Gerencia Operativa de Recursos Humanos (GORRHH, en adelante) u otra competente.

Asimismo, mediante el Compromiso de Confidencialidad el empleado declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 26 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

Se desarrollará un procedimiento para la suscripción del Compromiso de Confidencialidad donde se incluirán aspectos sobre:

- a) Suscripción inicial del Compromiso por parte de la totalidad del personal.
- b) Revisión del contenido del compromiso cada 12 meses máximo.

Los términos y condiciones de empleo establecerán la responsabilidad del empleado en materia de seguridad de la información y para la gestión de los activos del Organismo asociados con los sistemas de información y por los servicios manejados por los empleados, personal contratado o usuarios de tercera parte.

Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la sede del Organismo y del horario normal de trabajo, por ejemplo, en caso de trabajo en el hogar.

Los derechos y obligaciones del empleado relativos a la seguridad de la información, por ejemplo, en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de empleo.

7.2. Categoría: Durante el empleo

Objetivo de control

Asegurar que los empleados y personal contratado sean conscientes de sus responsabilidades con respecto a la seguridad de la información y las cumplan.


7.2.1. Responsabilidad de la Gerencia

Control

La dirección debe requerir a todos los empleados y personal contratado que apliquen la seguridad de la información de acuerdo con las políticas y los procedimientos establecidos por el Organismo.

Se deberá cumplir con lo siguiente:

- a) estar adecuadamente informados de sus roles y responsabilidades de seguridad de la información antes de que se le otorgue el acceso a información sensible o a los sistemas de información;
- b) ser provistos de guías para establecer las expectativas de seguridad de su rol dentro del Organismo;
- c) ser motivados para cumplir con las políticas de seguridad del Organismo;
- d) alcancen un nivel de conciencia sobre la seguridad acorde con sus roles y responsabilidades dentro del Organismo;
- e) cumplir con las condiciones y términos del empleo, los cuales incluyen las políticas de seguridad de la información del Organismo y métodos adecuados de trabajo;

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 27 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

f) mantenerse con las habilidades y calificaciones adecuadas.

Si los empleados, personal contratado y usuarios no son conscientes de sus responsabilidades de seguridad, ellos pueden causar daños considerables al Organismo. Un personal motivado tiene más probabilidades de ser más confiable y causar menos incidentes de seguridad de la información.

7.2.2. Concientización, formación y capacitación en seguridad de la información

Control

Todos los empleados del Organismo y, cuando sea pertinente el personal contratado, deben recibir una concientización, educación y capacitación apropiadas, y actualizaciones regulares sobre políticas y procedimientos organizacionales, que sean pertinentes a su tarea.

El titular de la GORRHH será el encargado de coordinar las acciones de capacitación que surjan de la presente Política. La capacitación de conocimientos deberá iniciarse con un proceso formal de inducción diseñado para introducir las políticas, expectativas y requerimientos de la seguridad del Organismo antes que se otorgue el acceso a la información o a los servicios. La capacitación incluirá además las responsabilidades legales y controles del Organismo, así también el correcto uso de las instalaciones y activos de procesamiento de la información.

Cada 12 meses como máximo, se revisará el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo al estado del arte de ese momento.


Por otra parte, se arbitrarán los medios técnicos necesarios para comunicar a todo el personal, eventuales modificaciones o novedades en materia de seguridad, que deban ser tratadas con un orden preferencial.

7.2.3. Proceso disciplinario

Control

Todo incumplimiento a la presente Política de Seguridad de la Información será investigado y tratado en el marco del Régimen de Investigaciones Administrativas -aprobado mediante el Decreto N°456/2022- y de conformidad con los principios, derechos y deberes reconocidos en el marco de la Ley N° 25.164 (Marco de Regulación de Empleo Público Nacional) y N°25.188 (de Ética en el Ejercicio de la Función Pública) en conjunto a sus respectivos Decretos Reglamentarios y toda otra normativa complementaria.

Se debe garantizar una respuesta adecuada, la cual debe tener en consideración factores como la naturaleza y gravedad del incidente, su impacto en el Organismo, si es la primera infracción o si es repetitivo, si el infractor ha sido o

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 28 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

no ha sido adecuadamente entrenado o informado de sus obligaciones y responsabilidades. En casos graves de mala conducta, el proceso deberá permitir la remoción urgente de las obligaciones de acceso y privilegios.

7.3. Categoría: Desvinculación o cambio de puesto

Objetivo de control

Proteger los intereses del Organismo como parte del proceso de desvinculación o cambio de puesto.

Se deben establecer las responsabilidades para asegurar que la salida del Organismo del usuario empleado, personal contratado o tercera persona sea manejada y se complete la devolución de todos los activos y/o elementos físicos que le fueron otorgados en el momento o durante su empleo o contratación, y se eliminen todos los derechos de acceso.


7.3.1. Responsabilidades en la desvinculación o cambio de puesto

Control

Se debe definir, comunicar y hacer cumplir, al empleado o personal contratado, las responsabilidades y las obligaciones relativas a la seguridad de la información que continúan vigentes luego de la desvinculación o cambio de puesto.

La comunicación de las responsabilidades en la desvinculación debe incluir los requisitos de seguridad de la información y las responsabilidades legales en curso y, cuando sea apropiado, las responsabilidades contenidas dentro de cualquier acuerdo de confidencialidad (ver 13.2.4), y los términos y condiciones de empleo (ver 7.1.2) debe continuar por un período de tiempo definido luego de la desvinculación del empleado o personal contratado.

El contrato del empleado o personal contratado debe contener las responsabilidades y deberes que permanecen válidos aún luego de la desvinculación (ver 7.1.2).

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 29 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

8. Cláusula: Gestión de Activos

Responsabilidad

El RSI es responsable de que los RPI clasifiquen los activos de acuerdo a su grado de criticidad, sensibilidad y de mantener actualizada y documentada su clasificación.

El RSI supervisará el proceso de clasificación y rotulado de la información.

El RSI y el RPI supervisarán el cumplimiento en el Organismo a empleados, personal contratado y usuarios de terceras partes de la presente Clausula.

Todo el personal del Organismo y usuarios de terceras partes serán responsables del cumplimiento de la presente Clausula.

8.1. Categoría: Responsabilidad por los Activos

Objetivo de control

Identificar los activos del Organismo y definir las responsabilidades apropiadas para su protección.

8.1.1. Inventario de activos

Control


Se deben identificar los activos asociados a la información y a las instalaciones de procesamiento de información y se debe elaborar y mantener un inventario de estos activos.

Se deberá identificar los activos relevantes en el ciclo de vida de la información, documentar y mantener un inventario de los activos más importantes, teniendo en cuenta la seguridad de la información. El ciclo de vida de la información deberá incluir la creación, elaboración, almacenamiento, transmisión, eliminación, destrucción y deposito final. La documentación deberá mantenerse en inventarios dedicados o existentes, según corresponda. El inventario de activos deberá ser exacto, actualizado, consistente y alineado con otros inventarios del Organismo.

Para cada uno de los activos identificados, deberá asignarse un responsable y deberá identificarse la clasificación. Los inventarios de activos ayudan a garantizar que se logre la protección eficaz.

El inventario de activos incluye:

- a) De Información: bases de datos, archivos de datos, documentación, contratos, acuerdos, Resoluciones, disposiciones, informes.
- b) De software: aplicaciones, sistemas, herramientas de desarrollo y utilitarios.
- c) Físicos: equipamiento de computación, equipamiento de comunicaciones, medios removibles y otros equipamientos.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 30 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- d) De servicios: aire acondicionado, energía, iluminación, protección contra incendio, y otros equipamientos.
- e) Instalaciones: edificios, ubicaciones físicas tendido eléctrico, de red de agua y gas etc.
- f) Recursos Humanos: Sus calificaciones, habilidades y experiencia.
- g) Intangibles: reputación e imagen del Organismo.

El inventario será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad no mayor a 12 meses.

El responsable de mantener actualizado el inventario es el RPI.

8.1.2. Responsabilidad de los Activos

Control

Los activos contenidos en el inventario deberán tener un responsable.

Los RPI son, según sus misiones y funciones, quienes deben cumplir con las siguientes responsabilidades:

- a) informar sobre cualquier cambio que afecte el inventario de activos;
- b) clasificar los activos en función a su valor, según la criticidad de la información soportada;
- c) definir los requisitos de seguridad de los activos;
- d) velar por la implementación y el mantenimiento de los controles de seguridad requeridos en los activos;
- e) revisar periódicamente, las restricciones y clasificaciones de acceso al activo, teniendo en cuenta las políticas de control de acceso aplicables.

La responsabilidad podría asignarse a:


- a) Un proceso de gestión
- b) Un conjunto definido de actividades
- c) Una aplicación
- d) Un conjunto de datos definidos

Cabe aclarar que, si bien los RPI pueden delegar la administración de sus funciones a personal idóneo a su cargo, conservarán la responsabilidad del cumplimiento de las mismas. La delegación de la administración por parte de los RPI de los activos será documentada por los mismos y proporcionada al RSI.

8.1.3. Uso aceptable de los activos

Control

Se deben identificar, documentar e implementar reglas para el uso aceptable de la información y los activos asociados a la información y a las instalaciones de procesamiento de la información.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 31 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

Los empleados, personal contratado, usuarios de tercera parte deben cumplir con las reglas para el uso aceptable de la información y los activos asociados con las instalaciones de procesamiento de esta, incluyendo:

- a) Regla para el uso del correo o internet.
- b) Guía para el uso de dispositivos móviles especialmente para el uso fuera del establecimiento o instalaciones del Organismo.

Se deberá concientizar a los empleados, personal contratado y los usuarios de tercera parte que utilizan o tienen acceso a los activos del Organismo, de sus límites existentes en el uso y manipulación de los activos y cumplir con los requisitos de seguridad para su protección y deben responsabilizarse del uso de los recursos asociados con las instalaciones de procesamiento de la información y de cualquier uso llevado a cabo bajo su responsabilidad.

Las reglas específicas, así como las guías y la concientización deberán ser previstas por la Subgerencia Operativa de Informática en conjunto con el Departamento de Capacitación de la GERENCIA OPERATIVA DE RECURSOS HUMANOS.

8.1.4. Retorno de los activos

Control

Todos los usuarios, tanto empleados como de terceras partes, deben devolver todos los activos del Organismo en su poder tras la terminación de su empleo, contrato o acuerdo.

El proceso de finalización deberá formalizarse para incluir la devolución de todos los activos físicos y electrónicos previamente emitidos pertenecientes o confiados al Organismo.

En los casos en que un empleado o usuario de tercera parte adquiere equipos del Organismo o utiliza su propio equipo, deberán seguirse procedimientos para garantizar que toda la información pertinente sea transferida al Organismo y borrada de forma segura del equipo.

En los casos en que un empleado o usuario de tercera parte tiene conocimiento de que es importante para las operaciones en curso, la información deberá documentarse y transferirse al Organismo.


8.2. Categoría: Clasificación de la información

Objetivo de control

Asegurar que la información reciba un nivel de protección apropiado de acuerdo con su importancia para el Organismo.

8.2.1. Clasificación de la información

Control

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 32 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

La información se debe clasificar en términos de los requisitos legales, su valor, criticidad y sensibilidad a la divulgación o modificación no autorizadas.

Se deberá clasificar la información, para indicar la necesidad, propiedades, el grado de protección esperado para cuando se trabaje con ella. Se utilizará un esquema de clasificación de la información para definir un conjunto apropiado de niveles de protección. El esquema de clasificación deberá incluir las convenciones para la clasificación y los criterios para la revisión de la clasificación en el tiempo. El nivel de protección en el esquema deberá evaluarse mediante el análisis de la confidencialidad, integridad y disponibilidad y cualquier otro requisito para la información considerada. El esquema deberá estar alineado con la política de control de acceso.

Cada nivel deberá tener un nombre que tenga sentido en el contexto de la aplicación del esquema de clasificación. El esquema deberá ser consistente en todo el Organismo para que todos clasifiquen la información y los activos relacionados de la misma manera, tengan un entendimiento común de los requisitos de protección y apliquen la protección adecuada. La clasificación deberá incluirse en los procesos del Organismo y deberá ser consistente y coherente en todo el Organismo. Los resultados de la clasificación deberán indicar el valor de los activos en función de su sensibilidad y criticidad para el Organismo, por ejemplo, en términos de confidencialidad, integridad y disponibilidad. Los resultados de la clasificación deberán actualizarse de acuerdo con los cambios de su valor, sensibilidad y criticidad durante su ciclo de vida.

La clasificación y los controles de protección asociados a la información deberán tener en cuenta que la gestión necesita compartir o restringir la información, así como los requisitos legales. Los activos que no son de información se pueden clasificar de conformidad con la clasificación de información que es almacenada, procesada o manipulada o protegida por el activo.


Los responsables de los activos de información son responsables de su clasificación.

8.2.2. Rotulado de la información

Control

Se debe desarrollar e implementar un conjunto apropiado de procedimientos para rotular la información de acuerdo con el esquema de clasificación de la información adoptado por el Organismo.

Los procedimientos para el etiquetado de la información necesitan cubrir la información y sus activos relacionados en formato físico y electrónico. El etiquetado deberá reflejar el esquema de clasificación establecido en 8.2. 1. Las etiquetas deberán reconocerse fácilmente. Los procedimientos deberán proporcionar orientación sobre dónde y cómo se adjuntan las etiquetas, considerando cómo se accede a la información o se gestionan los activos, en

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 33 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

función de los tipos de medios. Los procedimientos pueden definir casos en los que se omita el etiquetado, por ejemplo, el etiquetado de información no confidencial para reducir las cargas de trabajo. Los empleados y el personal contratado deberán estar al tanto de los procedimientos del etiquetado.

La salida de los sistemas que contienen información clasificada como sensible o crítica deberá llevar una etiqueta adecuada de clasificación.

El rotulado de la información clasificada es un requisito clave para acuerdos que impliquen compartir información. Los rótulos físicos son una forma común de identificación. De todas maneras, algunos activos de información como documentos en soporte digital no pueden ser rotulados físicamente y se hacen necesarios medios de identificación digital. Donde no es factible el rotulado, se podrán aplicar otros medios para designar la clasificación de la información, por ejemplo, vía procedimientos o vía metadatos.

Los acuerdos con otros Organismos o terceros partes que incluyan compartir información deben establecer los procedimientos para identificar la clasificación de dicha información y para interpretar los rótulos de clasificación de otros Organismos o terceras partes.

8.2.3. Manipulación de los activos

Control

Se deben desarrollar e implementar procedimientos para manipular la información de acuerdo con el esquema de clasificación de la información adoptado por el Organismo.

Deberán elaborarse procedimientos para el manejo, procesamiento, almacenamiento, comunicación desclasificación y destrucción de la información, de acuerdo con su clasificación (ver 8.2.1) y es conveniente que esto también incluya los procedimientos para la cadena de custodia y registro de cualquier evento de seguridad relevante.


8.3. Categoría: Manipulación de los medios

Objetivo de control

Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de la información almacenada en los medios.

8.3.1. Gestión de medios removibles

Control

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 34 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

Se deben implementar procedimientos para la gestión de medios removibles de acuerdo con el esquema de clasificación de la información adoptado por el Organismo.

Deberán considerarse las siguientes directrices para la gestión de medios extraíbles:

- a) si ya no son necesarios, los contenidos de los medios reutilizables que deberán retirarse del Organismo deberán hacerse irrecuperables;
- b) cuando sea necesario y práctico, deberá requerirse autorización para los medios a retirar del Organismo y deberá mantenerse un registro de dichas extracciones, a fin de mantener un registro de auditoría;
- c) todos los medios deberán almacenarse en un ambiente seguro, de acuerdo con las especificaciones del fabricante;
- d) si la confidencialidad o la integridad de los datos son consideraciones importantes, deberán utilizarse técnicas criptográficas para proteger los datos en los medios extraíbles;

El RSI implementará procedimientos para la administración de medios informáticos removibles como cintas, pen drives e informes impresos.

Se deben considerar las siguientes acciones para la implementación de los procedimientos:

- a) Eliminar de forma segura los contenidos, si ya no son requeridos de cualquier medio reutilizable que ha de ser retirado o reutilizado por el Organismo.
- b) Requerir autorización para retirar cualquier medio del Organismo y realizar un control de todos los retiros a fin de mantener un registro de auditoría.
- c) Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores y la criticidad de la información almacenada.


8.3.2. Disposición final de medios

Control

Cuando los medios dejen de ser requeridos, se deben eliminar de forma segura, utilizando procedimientos formales.

Deberán establecerse procedimientos formales para la eliminación segura de los medios para minimizar el riesgo de fuga de información confidencial a personas no autorizadas. Los procedimientos para la eliminación segura de los medios que contienen información confidencial deberán ser proporcionales a la sensibilidad de esa información. Deberán considerarse los siguientes elementos:

- a) los medios que contienen información confidencial deberán almacenarse y eliminarse de forma segura, por ejemplo, mediante incineración o

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 35 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

trituration, o el borrado de datos para su uso por otra aplicación dentro del Organismo;

- b) establecer procedimientos para identificar los elementos que puedan requerir la eliminación segura;
- c) puede ser más fácil organizar que todos los elementos de los medios sean recopilados y eliminados de forma segura, en lugar de tratar de separar los elementos sensibles;
- d) muchas organizaciones ofrecen servicios de recopilación y eliminación de los medios; se deberá tener cuidado en la selección de una tercera parte adecuada con los controles y experiencia adecuados;
- e) la eliminación de los elementos sensibles deberá registrarse a fin de mantener un registro de auditoría.

Cuando se acumulan medios para la eliminación, deberá tenerse en cuenta el efecto de agregación que puede causar que una gran cantidad de información no sensible se convierta en sensible.

Los procedimientos además deben considera que los siguientes elementos requerirán almacenamiento y eliminación segura:

- a) Documentos en papel.
- b) Voces u otras grabaciones.
- c) Papel carbónico.
- d) Informes de salida.
- e) Cintas de impresora de un solo uso.
- f) Cintas magnéticas.
- g) Discos u otros medios removibles.
- h) Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor).
- i) Listado de programas.
- j) Datos y/o listados de pruebas.
- k) Documentos del sistema.

Los dispositivos dañados que contienen datos sensibles pueden requerir una evaluación de riesgos para determinar si los elementos deberán ser destruidos físicamente en lugar de ser enviados para su reparación o descarte


La evaluación del mecanismo de eliminación, debe contemplar el tipo de dispositivo y la criticidad de la información contenida.

8.3.3. Traslado de medios físicos

Control

Los medios que contengan información se deben proteger contra accesos no autorizados, mal uso o corrupción durante el transporte.

Los procedimientos de transporte de medios informáticos entre diferentes puntos (envíos postales, mensajería, etc.) deben contemplar como mínimo:

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 36 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- a) La utilización de medios de transporte o servicios de mensajería confiables. El RSI a transportar determinará qué servicio de mensajería se utilizará conforme la criticidad de la información a transmitir.
- b) Suficiente embalaje para envío de medios a través de servicios postales o de mensajería, siguiendo las especificaciones de los fabricantes o proveedores.
- c) La adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas. Entre los ejemplos se incluyen:
 - 1) Uso de recipientes cerrados y rotulados.
 - 2) Entrega en mano.
 - 3) Embalaje a prueba de apertura no autorizada (que revele cualquier intento de acceso).
 - 4) En casos excepcionales, división de la mercadería a enviar en más de una entrega y envío por diferentes rutas.

9. Cláusula: Control de Accesos

Responsabilidad

El RSI será responsable de definir normas y procedimientos para: la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario; el monitoreo del uso de las instalaciones de procesamiento de la información; la solicitud y aprobación de accesos a Internet; el uso de computación móvil y reportes de incidentes relacionados; la respuesta a la activación de alarmas silenciosas; la revisión de registros de actividades (logs); y el ajuste de relojes de acuerdo a un estándar preestablecido.

También verificará la correcta implementación de las normas y procedimientos definidos en el control de accesos.


Los Responsables de las Áreas técnicas serán responsables de aplicar los controles definidos en conjunto con el RSI.

Los RPI serán responsables de evaluar los riesgos a los cuales se expone la información para determinar los controles de accesos, autenticación, utilización y registro de actividades a ser implementados en cada caso.

Aprobar y solicitar la asignación y revocación de privilegios a usuarios.

Los RPI junto con la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el CGS, definirán un cronograma de depuración de logs y registros de auditoría en línea en función a normas vigentes y a sus propias necesidades.

El CGS y los Jefes de Departamento, junto con el RSI, autorizarán el trabajo remoto - siempre y cuando la normativa vigente así lo habilite y en las condiciones establecidas al efecto- del personal a su cargo, en los casos en que se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 37 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

modo de cumplir con las normas vigentes. Asimismo, autorizarán el acceso de los usuarios a su cargo a los servicios y recursos de red y a Internet.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el CGS, tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

El CGS aprobará el análisis de riesgos de la información efectuado. Asimismo, aprobará el período definido para el mantenimiento de los registros de auditoría generados.

9.1. Categoría: Requisitos de la gestión para el control de accesos

Objetivo de control

Limitar el acceso a la información y a las instalaciones de procesamiento de Información.

9.1.1. Política de control de accesos

Control

Se debe establecer, documentar y revisar una política de control de accesos basada en los requisitos de la gestión y de la seguridad de la información.


En la aplicación de gestión de acceso, se contemplarán los siguientes aspectos:

- a) Identificar los requerimientos de seguridad de cada una de las aplicaciones.
- b) Identificar toda la información relacionada con las aplicaciones.
- c) Establecer criterios coherentes entre esta Política de Control de Acceso y la Política de Clasificación de Información de los diferentes sistemas según la cláusula de Gestión de Activos.
- d) Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
- e) Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.
- f) Administrar los derechos de acceso en un ambiente distribuido, que reconozcan todos los tipos de conexiones y dispositivos disponibles.

9.1.2. Acceso a las redes y a los servicios de red

Control

Se debe proveer a los usuarios solo el acceso a la red y a los servicios a los cuales han sido específicamente autorizados a utilizar.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 38 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

Debe redactarse un procedimiento relativo al use de redes y servicios de red. Este procedimiento debe cubrir:

- a) las redes y servicios de red a los cuales es permitido acceder;
- b) los procedimientos de autorización para determinar a quién se le permite el acceso a qué redes y qué servicios en red;
- c) los controles de gestión y procedimientos para proteger el acceso a las conexiones y servicios de red;
- d) los medios utilizados para acceder a las redes y servicios de red (por ejemplo, el uso de VPN o redes inalámbricas);
- e) los requisitos de autenticación del usuario para acceder a varios servicios de red;
- f) la supervisión del uso de los servicios de red.

9.2. Categoría: Gestión de Accesos de Usuario

Objetivo de control

Asegurar el acceso a los usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.


9.2.1. Alta y baja de registros de usuario

Control

Se debe implantar un proceso formal de alta y baja de registros del usuario para permitir la asignación de derechos de acceso.

El RSI definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual debe comprender:

- a) Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.
- b) Verificar que el usuario tiene autorización del RPI para el uso del sistema, base de datos o servicio de información.
- c) Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la PSI, por ejemplo, que no compromete la segregación de funciones.
- d) Entregar a los usuarios un detalle escrito de sus derechos de acceso.
- e) Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.
- f) Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 39 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- g) Mantener un registro formal de todas las personas registradas para utilizar el servicio.
- h) Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon del Organismo o sufrieron la pérdida/robo de sus credenciales de acceso.
- i) Efectuar revisiones periódicas con el objeto de:
 - 1) cancelar identificadores y cuentas de usuario redundantes.
 - 2) inhabilitar cuentas inactivas en un período no mayor a 60 días.
 - 3) eliminar cuentas inactivas en un período no mayor a 120 días.
- j) En el caso de existir excepciones, deben ser debidamente justificadas y aprobadas.
- k) Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.
- l) Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados en caso de corresponder.

9.2.2. Asignación de accesos del usuario


Control

Se debe implantar un proceso formal para otorgar o revocar los derechos de acceso a todos los tipos de usuario a todos los sistemas y servicios.

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema, resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

- a) Identificar los privilegios asociados a cada producto del sistema, por ejemplo, sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
- b) Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo, el requerimiento mínimo para su rol funcional.
- c) Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
- d) Establecer un período de vigencia para el mantenimiento de los privilegios (en base a la utilización que se le dará a los mismos) luego del cual los mismos serán revocados.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 40 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- e) Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

Los RPI serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el RSI.

9.2.3. Gestión de los derechos de acceso privilegiado

Control

Se debe restringir y controlar la asignación y uso de los derechos de acceso privilegiado.


En los diferentes ambientes de procesamiento existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como ser instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual.

El RSI definirá procedimientos para la administración de dichas contraseñas críticas que contemplen lo siguiente:

- a) Se definirán las causas que justificarán el uso de contraseñas críticas, así como el nivel de autorización requerido.
- b) Las contraseñas seleccionadas serán seguras, y su definición será efectuada como mínimo por dos personas, de manera que ninguna de ellas conozca la contraseña completa.
- c) Las contraseñas y los nombres de las cuentas críticas a las que pertenecen serán resguardadas debidamente.
- d) La utilización de las contraseñas críticas será registrada, documentando las causas que determinaron su uso, así como el responsable de las actividades que se efectúen con la misma.
- e) Cada contraseña crítica se renovará una vez utilizada y se definirá un período luego del cual la misma será renovada en caso de que no se la haya utilizado.
- f) Se registrarán todas las actividades que se efectúen con las cuentas críticas para luego ser revisadas. Dicho registro será revisado posteriormente por el RSI.

9.2.4. Gestión de la información secreta para la autenticación del usuario

Control

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 41 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

Se debe controlar la asignación de información secreta de autenticación a través de un proceso formal de gestión.

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

- a) Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo. Esta declaración bien puede estar incluida en el Compromiso de Confidencialidad.
- b) Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisionales, que se asignan cuando los usuarios olvidan su contraseña, sólo deben suministrarse una vez acreditada la identidad del usuario.
- c) Generar contraseñas provisionales seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo formal cuando la reciban.
- d) Almacenar las contraseñas sólo en sistemas informáticos protegidos.
- e) Utilizar otras tecnologías de autenticación y autorización de usuarios, como ser la biométrica (por ejemplo, verificación de huellas dactilares), verificación de firma, uso de autenticadores de hardware (como las tarjetas de circuito integrado), etc. El uso de esas herramientas se dispondrá cuando la evaluación de riesgos realizada por el RSI conjuntamente con quien ejerza la titularidad de la Subgerencia Operativa de informática y el RPI lo determine necesario (o lo justifique).
- f) Definir un procedimiento que establezca fortaleza de las contraseñas, bloqueo de acceso por cantidad de intentos fallidos, periodos de cambio de contraseñas y reutilización de las mismas.


9.2.5. Revisión de los derechos de acceso del usuario

Control

Los responsables de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el RPI definirá un procedimiento para revisar los derechos de acceso de los usuarios, el cual debe contemplar:

- a) Intervalos a revisar los derechos de acceso de los usuarios.
- b) Intervalos a revisar las autorizaciones de privilegios especiales de derechos de acceso.
- c) Intervalos a revisar las asignaciones de privilegios, a fin de garantizar que no se obtengan privilegios no autorizados.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 42 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

9.2.6. Remoción o ajuste de los derechos de acceso

Control

Se deben eliminar tras la finalización de su empleo, contrato o acuerdo, o se deben ajustar a cualquier cambio, los derechos de acceso a la información y a las instalaciones de procesamiento de la información de todos los usuarios, tanto empleados como de terceras partes.

Deberá redactarse un procedimiento que determine la remoción de los derechos otorgados a un individuo tras su desvinculación del Organismo. Este procedimiento debe contemplar los cambios en la relación laboral, la remoción de los derechos debe incluir accesos físicos y lógicos.

La remoción o el ajuste se pueden hacer mediante la remoción o la revocación o el reemplazo de las claves, tarjetas de identificación, instalaciones de procesamiento de información o suscripciones. Cualquier documentación que identifique los derechos de acceso de los empleados y personal contratado deberá reflejar la remoción o el ajuste de los derechos de acceso. Si un empleado o usuario de tercera parte que se marcha ha conocido las contraseñas para ID de usuarios que permanecen activos, estas deberán cambiarse al momento de la desvinculación o cambio de cargo, contrato o acuerdo.

Los derechos de acceso a la información y los activos asociados con las instalaciones de procesamiento de información, deberán reducirse o removerse antes de que el empleo termine o cambie, dependiendo de la evaluación de los factores de riesgo tales como:

- a) si la desvinculación o cambio es iniciado por el empleado, usuario de terceras partes, o por la dirección y la razón de la desvinculación;
- b) las responsabilidades actuales del empleado, parte usuaria de tercera parte o cualquier otro usuario;
- c) el valor de los activos accesibles actualmente.


9.3. Categoría: Responsabilidades del usuario

Objetivo de control

Hacer a los usuarios responsables de custodiar su información para la autenticación.

La cooperación de los usuarios autorizados es esencial para una seguridad efectiva.

Los usuarios deben estar al tanto de sus responsabilidades para mantener controles de acceso efectivos, particularmente con relación al uso de claves secretas y la seguridad del equipo del usuario.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 43 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

Se debe implementar una política de escritorio y pantalla limpios para reducir el riesgo de acceso no autorizado o daño a los papeles, medios y medios de procesamiento de la información.

9.3.1. Uso de la información secreta para la autenticación

Control

Se debe solicitar a los usuarios que sigan las prácticas del Organismo referidas al uso de la información secreta para la autenticación.


Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

- a) Mantener las contraseñas en secreto.
- b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- c) Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el RPI de que se trate, que:
 - 1) Sean fáciles de recordar.
 - 2) No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo, nombres, números de teléfono, fecha de nacimiento, etc.
 - 3) No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.
- d) Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
- e) Cambiar las contraseñas provisionales en el primer inicio de sesión (“log on”).
- f) Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
- g) Notificar de acuerdo a lo establecido en la Cláusula de Gestión de los Incidentes de Seguridad de la información, cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se notificará a los mismos que

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 44 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

pueden utilizar una única contraseña para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas y en tránsito.

9.4. Categoría: Control de acceso a los sistemas y a las aplicaciones

Objetivo de control

Prevenir el acceso no autorizado a los sistemas y las aplicaciones.

9.4.1. Restricción de acceso a la información

Control

Se debe restringir el acceso a la información y a las funciones de los sistemas de aplicaciones de acuerdo con la política de control de acceso.

Las restricciones al acceso deben basarse en los requisitos de aplicación individual y estar de acuerdo con la política de control de acceso definida.

Deberá considerarse lo siguiente para dar soporte a los requisitos de restricción de acceso:

- a) proveer menús para controlar el acceso a las funciones del sistema de aplicaciones;
- b) controlar los datos que pueden ser accedidos por un usuario particular;
- c) Controlar los derechos de acceso de los usuarios, por ejemplo, leer, escribir, borrar y ejecutar;
- d) controlar los derechos de acceso a otras aplicaciones;
- e) limitar la información contenida en las salidas;
- f) proporcionar controles de acceso físico o lógico para el aislamiento de las aplicaciones sensibles, datos de aplicación o sistemas

9.4.2. Procedimientos seguros de inicio de sesión


Control

Se debe controlar el acceso a los sistemas y a las aplicaciones mediante un procedimiento seguro de inicio de sesión, cuando lo requiera la política de control de acceso.

Deberá elegirse una técnica de autenticación adecuada para justificar la identidad de un usuario.

Cuando se requiere una fuerte autenticación y verificación de la identidad, deberán utilizarse métodos alternativos a las contraseñas, tales como medios criptográficos, tarjetas inteligentes o medios biométricos.

El procedimiento para iniciar sesión en un sistema o aplicación deberá ser diseñado para minimizar la oportunidad de acceso no autorizado. Por lo tanto, el proceso de conexión (log-on) deberá divulgar el mínimo de información sobre el

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 45 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

sistema o aplicación, de manera de evitar proveer a un usuario no autorizado con asistencia innecesaria. Un buen procedimiento de conexión (log-on) deberá:

- a) no mostrar identificación del sistema o aplicación hasta que termine el proceso de conexión;
- b) desplegar un mensaje genérico advirtiendo que el sistema deberá accederse solamente por usuarios autorizados;
- c) no ofrecer mensajes de ayuda durante el proceso de conexión (log - on) que puedan guiar a usuarios no autorizados;
- d) validar la información de conexión (log-on) sólo tras rellenar todos sus datos de entrada.
- e) Si se produce una condición de error, el sistema no deberá indicarse qué parte de esos datos es correcta o incorrecta;
- f) proteger contra intentos de inicio de sesión por fuerza bruta;
- g) registrar los intentos fallidos y exitosos de conexión;
- h) provocar un evento de seguridad si se detecta una posible violación fallida o exitosa de los controles de inicio de sesión;
- i) mostrar la siguiente información tras completar una conexión con éxito:
 - 1) fecha y hora de la anterior conexión (log-on) realizada con éxito;
 - 2) detalles de cualquier intento de conexión fallido desde el momento de la última conexión realizada con éxito.
- j) no mostrar la contraseña que está siendo ingresada;
- k) no transmitir por una red contraseñas en texto limpio;
- l) terminar sesiones inactivas después de un período de inactividad definido, especialmente en las ubicaciones de alto riesgo tales como en las áreas públicas o externas fuera de la gestión de seguridad de la información o en los dispositivos móviles;
- m) restringir los tiempos de conexión para proporcionar seguridad adicional para aplicaciones de alto riesgo y reducir la ventana de oportunidades para el acceso no autorizado.


9.4.3. Sistema de gestión de contraseñas

Control

Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.

El sistema de gestión de contraseñas deberá:

- a) imponer el uso de contraseñas e identificaciones de usuario (IDs) individuales con el fin de establecer responsabilidades;
- b) permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación para evitar errores al introducirlas;
- c) imponer la selección de contraseñas de calidad;

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 46 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- d) forzar a los usuarios el cambio de contraseñas temporarias en su primera conexión (logon);
- e) aplicar los cambios de contraseña normales, y según sea necesario;
- f) mantener un registro de las anteriores contraseñas utilizadas, e impedir su reutilización;
- g) no mostrar las contraseñas en la pantalla cuando se están introduciendo;
- h) almacenar archivos de contraseñas en lugares diferentes de los datos del sistema de aplicaciones;
- i) almacenar y transmitir las contraseñas en formatos protegidos.

9.4.4. Uso de herramientas con privilegios

Control

Se debe restringir y controlar rigurosamente el uso de herramientas que podrían ser capaces de pasar por alto los controles del sistema o de las aplicaciones.

Deberán considerarse las siguientes directrices y controles de aplicación para el uso de programas de utilidad que podrían ser capaces de anular el sistema:


- a) el uso procedimientos de identificación, autenticación y autorización para los programas de utilidad;
- b) la separación de los programas de utilidad de las aplicaciones de software;
- c) la limitación de la utilización de programas de utilidad para el número práctico mínimo de los usuarios autorizados y de confianza (ver 9.2.2);
- d) la autorización para el uso especial de los programas de utilidad;
- e) la limitación de la disponibilidad de los programas de utilidad, por ejemplo, para la autorización de un cambio no autorizado;
- f) el registro de todo el uso de los programas de servicios públicos;
- g) la definición y documentación de los niveles de autorización para los programas de utilidad;
- h) la eliminación o desactivación de todos los programas de utilidad innecesarios;
- i) no poner a disposición de los usuarios los programas de utilidad que tienen acceso a las aplicaciones en sistemas donde se requiere la separación de funciones.

9.4.5. Control de acceso al código fuente de los programas

Control

Se debe restringir el acceso al código fuente de los programas.

El acceso al código de programas fuente y artículos asociados (como diseños, especificaciones, proyectos de verificación y proyectos de validación) deberá ser

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 47 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

estrictamente controlado, para prevenir la introducción de una funcionalidad no autorizada, evitar cambios involuntarios, así como a mantener la confidencialidad de la propiedad intelectual valiosa. Para el código de programas fuente, esto puede alcanzarse por almacenamiento centralizado controlando dicho código, preferentemente en las bibliotecas de programas fuentes. Las directrices siguientes deberán ser consideradas para controlar el acceso a tales bibliotecas de programas fuente y para reducir el potencial de corrupción de programas:

- a) de ser posible, las bibliotecas de programas fuente no deberán ser soportadas en sistemas de producción;
- b) el código de programas fuente y las bibliotecas de programas fuente deberán gestionarse según procedimientos establecidos;
- c) el personal de apoyo deberá tener acceso restringido a bibliotecas de programas fuente;
- d) la actualización de bibliotecas de programas fuente y artículos asociados, y la entrega de programas fuente a programadores sólo deberá realizarse después de que la autorización apropiada ha sido recibida;
- e) los listados de programas deberán mantenerse en un ambiente seguro;
- f) deberá mantenerse un registro de auditoría de todos los accesos a bibliotecas de programas fuente;
- g) el mantenimiento y la copia de bibliotecas de programas fuente deberán estar sujetos a procedimientos estrictos de control de cambio (ver 14.2.2).

Si el código fuente del programa va a ser publicado deberán considerarse controles adicionales para ayudar a conseguir garantías sobre su integridad (por ejemplo, la firma digital).


10. Cláusula: Criptografía

Responsabilidad

El RSI, junto con los RPI definirá en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Luego, junto a las áreas técnicas intervinientes, se definirán los métodos de encriptación a ser utilizados.

El RSI cumplirá las siguientes funciones:

- Definir los procedimientos de administración de claves.
- Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.
- Garantizar el cumplimiento de los requerimientos de seguridad para el software.
- Definir procedimientos para: el control de cambios a los sistemas; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas; el control de código malicioso; y la definición de las funciones del personal involucrado en el proceso de entrada de datos.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 48 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- Identificar el nivel requerido de protección, tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar.

10.1. Categoría: Criptografía

Objetivo de control

Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información.

10.1.1. Política de uso de controles criptográficos

Control

Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.


Se debe tener en cuenta las siguientes consideraciones en el desarrollo de una norma criptográfica:

- a) El enfoque de dirección del CGS hacia el empleo de controles criptográficos a través del Organismo, incluyendo los principios generales bajo los cuales la información de gestión debe ser protegida;
- b) Basado en una evaluación de riesgo, el nivel requerido de protección deberá ser identificado teniendo en cuenta el tipo, la fuerza, y la calidad del algoritmo de cifrado requerido;
- c) El empleo de cifrado para protección de información transportada por medios removibles, por dispositivos móviles o a través de líneas de comunicación;
- d) Un enfoque de gestión de claves, incluyendo métodos para tratar la protección de claves criptográficas y la recuperación de información cifrada en el caso de claves perdidas, comprometidas o dañadas;
- e) El impacto de usar información cifrada, sobre los controles que centran en la inspección de contenido (por ejemplo, la detección de software malicioso).

Al implementar la presente norma de criptografía, deberán considerarse las regulaciones y las restricciones nacionales que podrían aplicarse al empleo de técnicas criptográficas en las diferentes partes del mundo y las cuestiones de pasaje de frontera de transacciones de información cifrada.

Los controles criptográficos pueden ser usados para alcanzar diferentes objetivos de seguridad, por ejemplo:

- a) *Confidencialidad:* utilización de cifrado de información para proteger información sensible o crítica, almacenada o transmitida;

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 49 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- b) *Integridad/autenticidad:* la utilización de firmas digitales o códigos de autenticación de mensaje para proteger la autenticidad y la integridad de la información sensible o crítica almacenada o transmitida;
- c) *No repudio:* utilización de técnicas criptográficas, para obtener pruebas del suceso o no de un acontecimiento o acción;
- d) *Autenticación:* utilizar técnicas criptográficas para autenticar a los usuarios y otras entidades del sistema que soliciten acceso o realizar transacciones con otros usuarios, entidades y recursos del sistema

10.1.2. Gestión de Claves

Control

Se debe desarrollar e implementar una política sobre el uso, protección y vida útil de las claves criptográficas a lo largo de todo su ciclo de vida.

Deberán definirse los requisitos para la gestión de claves criptográficas en todo su ciclo de vida, incluyendo la generación, el almacenamiento, el archivo, la recuperación, la distribución, el retiro y la destrucción de las claves.


Deberán seleccionarse los algoritmos criptográficos, las longitudes de las claves y las prácticas de uso de acuerdo a las mejores prácticas. La gestión de claves adecuada requiere procesos seguros para la generación, el almacenamiento, el archivo, la recuperación, la distribución, el retiro y la destrucción de las claves.

Todas las claves criptográficas deberán ser protegidas contra la modificación y la pérdida.

Además, claves secretas y privadas necesitan la protección contra el uso no autorizado, así como contra la divulgación. El equipo para generar, almacenar y archivar claves deberá ser protegido físicamente.

El sistema de gestión de claves deberá estar basado en un conjunto reconocido de normas, procedimientos, y métodos seguros para:

- a) generar claves para sistemas criptográficos diferentes y aplicaciones diferentes;
- b) generar y obtener certificados de clave pública;
- c) distribuir claves a las entidades que corresponda, incluyendo cómo deberán activarse las claves al recibirse;
- d) almacenar claves, incluyendo cómo los usuarios autorizados obtienen el acceso a las claves;
- e) cambiar o actualizar claves, incluyendo reglas sobre cuándo las claves deberán ser cambiadas y cómo esto deberá hacerse;
- f) tratar las claves comprometidas;
- g) revocar claves incluyendo como deberán retirarse o desactivarse las mismas, por ejemplo, cuando las claves están comprometidas o cuando un usuario se desvincula del Organismo (en cuyo caso las claves también deberán archivarse);

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 50 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- h) recuperar claves que se han perdido o corrompido;
- i) archivar o respaldar claves;
- j) destruir claves;
- k) registrar y auditar las actividades relacionadas con la gestión de claves.

Para reducir la probabilidad de uso inadecuado, las fechas de activación y desactivación de claves deberán ser definidas de modo que las claves sólo puedan ser usadas durante un período limitado de tiempo definido en la política de gestión de claves asociada.

Además de la gestión segura de claves públicas y privadas, la autenticidad de claves públicas también deberá ser considerada. Este proceso de autenticación puede ser hecho usando los certificados de clave pública que normalmente son emitidos por una autoridad de certificación, que deberá ser una organización aprobada con controles y procedimientos adecuados para proporcionar el grado de confiabilidad requerido.

Los contenidos de los acuerdos de nivel de servicio o de los contratos con los proveedores externos de servicios criptográficos, por ejemplo, una autoridad certificadora, deberá cubrir los aspectos de las responsabilidades, fiabilidad de los servicios y tiempos de respuesta para la prestación de los mismos.

11. Cláusula: Protección Física y del Entorno

Responsabilidad

El RSI definirá junto con los RPI según corresponda, las medidas de protección física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos, y controlará su implementación. Asimismo, verificará el cumplimiento de las disposiciones sobre la protección física y ambiental indicada en la presente.


El RPI correspondiente asistirá, en la definición de las medidas de seguridad a implementar en áreas protegidas, y coordinará su implementación. Asimismo, controlará el mantenimiento del equipamiento informático de acuerdo a las indicaciones de proveedores tanto dentro como fuera de las instalaciones del Organismo.

El RSI junto al RPI correspondiente, definirá los niveles de acceso físico del personal del Organismo a las áreas restringidas bajo su responsabilidad.

El RSI junto al RPI correspondiente, autorizarán formalmente el trabajo fuera de las instalaciones con información de su incumbencia a los empleados del Organismo cuando lo crean conveniente.

La Auditoría Interna o en su defecto quien sea propuesto por el CGS revisará los registros de acceso a las áreas protegidas.

Todo el personal del Organismo, personal contratado y usuarios de terceras partes serán responsables del cumplimiento del presente capítulo.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 51 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

11.1. Categoría: Áreas seguras

Objetivo de control

Impedir accesos físicos no autorizados, daños e interferencia a la información y a las instalaciones de procesamiento de información del Organismo.

11.1.1. Perímetro de seguridad física

Control


Se deberá definir y usar perímetros de seguridad para proteger áreas que contengan información e instalaciones de procesamiento de información sensibles o críticas.

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de las sedes del Organismo y de las instalaciones de procesamiento de información.

El Organismo utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. Un perímetro de seguridad está delimitado por una barrera, por ejemplo, una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada barrera estarán definidas por el RSI.

Se considerarán e implementarán los siguientes lineamientos y controles, según corresponda:

- a) Definir y documentar claramente el perímetro de seguridad.
- b) Ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida (por ejemplo, no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser sólidas y todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados, por ejemplo, mediante mecanismos de control, vallas, alarmas, cerraduras, etc.
- c) Verificar la existencia de un área de recepción atendida por personal. Si esto no fuera posible se implementarán los siguientes medios alternativos de control de acceso físico al área o edificio. El acceso a dichas áreas y edificios estará restringido exclusivamente al personal autorizado. Los métodos implementados registrarán cada ingreso y egreso en forma precisa.
- d) Extender las barreras físicas necesarias desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo, por incendio, humedad e inundación.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 52 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- e) Identificar claramente todas las puertas de incendio de un perímetro de seguridad.

Un área segura puede ser una oficina con llave, o varias oficinas rodeadas por una barrera de seguridad física interna continua. Pueden ser necesarios barreras y perímetros adicionales para controlar el acceso físico entre las áreas con diferentes requerimientos de seguridad, dentro del mismo perímetro de seguridad

EL RSI junto con el RPI correspondiente, llevarán un registro actualizado de los sitios protegidos, indicando:

- a) Identificación del Edificio y Área.
- b) Principales elementos a proteger.
- c) Medidas de protección física


11.1.2. Controles de ingreso físico

Control

Se deben proteger las áreas seguras mediante controles de ingreso apropiados para asegurar que solo se permita el acceso al personal autorizado.

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por RSI junto con el RPI correspondiente, a fin de permitir el acceso sólo al personal autorizado. Estos controles de acceso físico tendrán, por lo menos, las siguientes características:

- a) Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia.
- b) Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se utilizarán controles de autenticación para autorizar y validar todos los accesos y se mantendrá un registro protegido para permitir auditar todos los accesos.
- c) Implementar el uso de una identificación unívoca visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.
- d) Revisar y actualizar en un período no mayor a 6 meses, los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el RPI correspondiente.
- e) Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará la auditoría Interna o en su defecto quien sea propuesto por el CGS.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 53 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

11.1.3. Aseguramiento de oficinas, recintos, instalaciones

Control


Se debe diseñar y aplicar la seguridad física a las oficinas, recintos e instalaciones.

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo, se considerarán las amenazas a la seguridad que representan los edificios y zonas aledañas, por ejemplo, filtración de agua desde otras instalaciones. Se definen los siguientes sitios como áreas protegidas del Organismo.

Áreas Protegidas

Se establecen las siguientes medidas de protección para áreas protegidas:

- a) Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.
- b) Establecer que los edificios o sitios donde se realicen actividades de procesamiento de información serán discretos y ofrecerán un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.
- c) Ubicar las funciones y el equipamiento de soporte, por ejemplo: impresoras, fotocopiadoras, máquinas de fax, adecuadamente dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información.
- d) Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia. Se agregará protección externa a las ventanas, en particular las que se encuentran en planta baja o presenten riesgos especiales.
- e) Implementar mecanismos de control para la detección de intrusos. Los mismos serán instalados según estándares profesionales y probados periódicamente. Estos mecanismos de control comprenderán todas las puertas exteriores y ventanas accesibles.
- f) Separar las instalaciones de procesamiento de información administradas por el Organismo de aquellas administradas por terceros.
- g) Restringir el acceso público a las guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible.
- h) Almacenar los materiales peligrosos o combustibles en los siguientes lugares seguros a una distancia prudencial de las áreas protegidas del Organismo. Los suministros, como los útiles de escritorio, no serán trasladados al área protegida hasta que sean requeridos.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 54 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- i) Almacenar los equipos redundantes y la información de resguardo (back up) en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal.

11.1.4. Protección contra amenazas externas y del entorno

Control

Se debe diseñar y aplicar la protección física contra desastres naturales, ataques intencionales o accidentes.

Se deberá asignar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre.

Se debe prestar consideración a cualquier amenaza contra la seguridad presentada por locales vecinos; por ejemplo, un fuego en un edificio vecino, escape de agua en el techo o pisos en sótano o una explosión en la calle.

Se deberán considerar los siguientes lineamientos para evitar el daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre:

- a) los materiales peligrosos o combustibles deben ser almacenados a una distancia segura del área asegurada. Los suministros a granel como papelería no deben almacenarse en el área asegurada;
- b) el equipo de reemplazo y los medios de respaldo debieran ubicarse a una distancia segura para evitar el daño de un desastre que afecte el local principal;
- c) se debe proporcionar equipo contraincendios ubicado adecuadamente.


11.1.5. Trabajo en áreas seguras

Control

Se debe diseñar y aplicar procedimientos para el trabajo en áreas seguras.

Para incrementar la seguridad de las áreas, se establecerán controles y lineamientos adicionales. Incluye controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí:

- a) Dar a conocer al personal la existencia del área protegida, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.
- b) Evitar la ejecución de trabajos por parte de terceros sin supervisión.
- c) Bloquear físicamente e inspeccionar periódicamente las áreas protegidas desocupadas.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 55 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- d) Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso, como el de cualquier otra persona ajena que requiera acceder al área protegida, será otorgado solamente cuando sea necesario y se encuentre autorizado y monitoreado. Se mantendrá un registro de todos los accesos de personas ajenas.
- e) Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.
- f) Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, a menos que hayan sido formalmente autorizadas por el RSI o el RPI correspondiente.
- g) Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información.

11.1.6. Áreas de carga y descarga

Control

Se deben controlar los puntos de acceso, tales como las áreas de carga y descarga y otros puntos donde personas no autorizadas puedan llegar a entrar a las instalaciones y de ser posible se deben aislar de las instalaciones de procesamiento de información para evitar el acceso no autorizado.


Se controlarán las áreas de carga y descarga las cuales estarán aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados.

Para ello se establecerán controles físicos que considerarán los siguientes lineamientos:

- a) Limitar el acceso a las áreas de depósito, desde el exterior de la sede del Organismo, sólo al personal previamente identificado y autorizado.
- b) Diseñar el área de depósito de manera tal que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio.
- c) Proteger todas las puertas exteriores del depósito cuando se abre la puerta interna.
- d) Inspeccionar el material entrante para descartar peligros potenciales antes de ser trasladado desde el área de depósito hasta el lugar de uso.
- e) Registrar el material entrante al ingresar al sitio pertinente.
- f) Cuando fuese posible, el material entrante debe estar segregado o separado en sus diferentes partes que lo constituyan.

11.2. Categoría: Equipamiento

Objetivo de control

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 56 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

Impedir la pérdida, el daño, el robo o el compromiso de los activos, así como la interrupción de las operaciones del Organismo.

11.2.1. Ubicación y protección del equipamiento

Control

Se debe ubicar y proteger el equipamiento de manera tal que se reduzcan los riesgos ocasionados por amenazas y peligros del entorno y las oportunidades de acceso no autorizado.


El equipamiento deberá ser ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos:

- a) Ubicar el equipamiento en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.
- b) Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.
- c) Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.
- d) Adoptar controles para minimizar el riesgo de amenazas físicas potenciales, por ejemplo: Robo, incendio, explosivos, humo, agua (inundación o falta de suministro), polvo, vibraciones, efectos químicos, interferencia en el suministro de energía eléctrica, interferencia en las comunicaciones, radiaciones electromagnéticas y vandalismo. Considerando tener en cuenta, además, el impacto de las amenazas citadas en zonas próximas a la sede del Organismo.
- e) Se deben establecer lineamientos sobre las actividades de comer, beber y fumar en la proximidad de los medios de procesamiento de la información.
- f) supervisar y controlar las condiciones ambientales como la temperatura y humedad para evitar que estas condiciones puedan afectar de manera adversa la operación de las instalaciones de procesamiento de información.
- g) Se deben aplicar protección contra rayos a todos los edificios y se deben adaptar filtros de protección contra rayos a todas las líneas de ingreso de energía y comunicaciones.

11.2.2. Elementos de soporte

Control

Se debe proteger el equipamiento de fallas en el suministro eléctrico o de otras interrupciones ocasionadas por fallas en elementos de soporte.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 57 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

El equipamiento estará protegido con respecto a las posibles fallas en el suministro eléctrico u otras interrupciones ocasionadas por fallas de elementos de soporte. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía.


Se contemplarán las siguientes medidas:

- a) Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.
- b) Contar con un suministro de energía interrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas del Organismo.
- c) La determinación de dichas operaciones críticas, será el resultado del análisis de impacto realizado por el RSI conjuntamente con los RPI con incumbencia. Los planes de contingencia contemplarán las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS serán inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.
- d) Montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Debe realizarse un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento, con el objeto de definir qué componentes será necesario abastecer de energía alternativa. Dicho análisis será realizado por el RSI conjuntamente con los RPI. Se dispondrá de un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado. Cuando el encendido de los generadores no sea automático, se asegurará que el tiempo de funcionamiento de la UPS permita el encendido manual de los mismos. Los generadores serán inspeccionados y probados periódicamente para asegurar que funcionen según lo previsto.

Asimismo, se procurará que los interruptores de emergencia se ubiquen cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica. Se proveerá de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía. Se implementará protección contra descargas eléctricas en todos los edificios y líneas de comunicaciones externas de acuerdo a las normativas vigentes.

Las opciones para lograr la continuidad de los suministros de energía incluyen múltiples alimentaciones para evitar que una falla en el suministro de energía.

Se debe controlar que el abastecimiento del agua sea estable y adecuado para el funcionamiento de los aires acondicionados, los equipos de humidificación y los sistemas de extinción de fuego (cuando se utilicen). Se debe evaluar la instalación de un sistema de alarma o aviso para detectar funcionamiento defectuoso o falla en los elementos de soporte.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 58 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

11.2.3. Seguridad del cableado

Control

El cableado de energía eléctrica y de telecomunicaciones que transporta datos o que da soporte a los servicios de información se debe proteger de intercepciones, interferencias o daños.

Acciones para su protección:


- a) Cumplir con los requisitos técnicos vigentes de la República Argentina.
- b) Utilizar piso-ducto o cableado embutido en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información. En su defecto estarán sujetas a la protección alternativa que se definirá en un procedimiento para tal fin.
- c) Proteger el cableado de red contra intercepción no autorizada o daño mediante controles como el uso de conductos o evitando trayectos que atraviesen áreas públicas.
- d) Separar los cables de energía de los cables de comunicaciones para evitar interferencias.
- e) Proteger el tendido del cableado troncal (backbone) mediante la utilización de ductos blindados.
- f) Para los sistemas sensibles o críticos que se identificaran en un procedimiento, se implementarán los siguientes controles adicionales:
 - a) Instalar conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección.
 - b) Utilizar rutas o medios de transmisión alternativos.
 - c) Acceso controlado a los paneles de comunicación y salas de conexión y cableado.
- g) Que se utilicen cables claramente identificables y marcas de equipos para minimizar el manejo erróneo, como el armado erróneo de los cables de red.
- h) Confeccionar y utilizar una lista documentada actualizada de conexiones para reducir la posibilidad de errores.
- i) Uso de cableado de fibra óptica.
- j) Uso de protección electromagnética para proteger el cableado.
- k) Realización de barridos técnicos e inspecciones físicas periódicas para buscar dispositivos que hayan sido acoplados a los cables sin autorización.

11.2.4. Mantenimiento del equipamiento

Control

El equipamiento debe recibir un mantenimiento correcto para asegurar su continua disponibilidad e integridad.

- a) Someter el equipamiento y elementos de soporte a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 59 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

especificaciones recomendados por el proveedor y con la autorización formal del RSI. El Área de seguridad mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.

- b) Se establece que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
- c) Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
- d) Autorizar y registrar el retiro de equipamiento o de componentes de la sede del Organismo para su mantenimiento.
- e) Eliminar la información confidencial, según la clasificación definida como la marca la norma de clasificación de la información, que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.
- f) Se debe cumplir con todos los requerimientos impuestos por la presente política.

11.2.5. Retiro de activos

Control

No se debe retirar del sitio equipamiento información o software sin previa autorización.

Sin tener en cuenta quien sea el responsable del equipamiento, la información y el software no serán retirados de la sede del Organismo sin autorización formal del RSI. Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos del Organismo, las que serán llevadas a cabo por el RPI. El personal será puesto en conocimiento de la posibilidad de realización de dichas comprobaciones.


Los empleados deben saber que se llevan a cabo controles inesperados, y los controles se deben realizar con la debida autorización de los requerimientos legales y reguladores.

Los empleados, personal contratado y usuarios de terceras partes quienes tienen autoridad para permitir la remoción o retiro de los activos fuera del Organismo deben ser claramente identificados y deben cumplir con los requerimientos de seguridad para protección de los activos del Organismo.

11.2.6. Seguridad del equipamiento y los activos fuera de la organización.

Control

Se debe aplicar seguridad a los activos fuera del Organismo teniendo en cuenta los diferentes riesgos de trabajar fuera de sus instalaciones.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 60 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito del Organismo, será autorizado por el RSI. En el caso de que en el mismo se almacene información clasificada, debe ser aprobado además por el responsable de la misma. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito del Organismo para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

Se respetarán permanentemente las instrucciones del fabricante respecto del cuidado del equipamiento.

Asimismo, se mantendrá una adecuada cobertura de seguro para proteger el equipamiento fuera del ámbito del Organismo, cuando sea conveniente.

Los riesgos de seguridad, por ejemplo: daño, robo o interceptación; puede variar considerablemente según las ubicaciones por ello, se debe evaluar los controles más apropiados, se debe tener en cuenta como mínimo el equipamiento y dispositivos retirados del ámbito del Organismo estén correctamente identificados, rotulados y no permanezca desatendido en lugares públicos.

Las computadoras personales deben ser además disimuladas y/o enmascaradas durante su viaje o transporte.

11.2.7. Disposición final segura o reutilización del equipamiento

Control

Se debe verificar todos los componentes del equipamiento que contengan medios de almacenamiento para asegurar que antes de su disposición final o reutilización se haya eliminado o sobrescrito de manera segura cualquier dato sensible y software licenciado.

Los dispositivos o medios de almacenamiento que contengan información sensible serán destruidos, borrados o sobrescritos en forma segura usando técnicas para que la información original sea irrecuperable.


Los dispositivos o medios de almacenamiento que contengan información confidencial deben requerir una evaluación de riesgo para determinar si debieran ser físicamente destruidos en lugar de enviarlos a reparar o descartar.

11.2.8. Equipamiento desatendido de usuario

Control

Los usuarios deben asegurar que el equipamiento desatendido tenga la protección apropiada.

El RPI debe informar a todos los usuarios y al personal contratado, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 61 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

desatendidos, así como de sus funciones en relación a la implementación de dicha protección.

11.2.9. Política de escritorio y de pantalla limpios


Control

Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procesamiento de la información.

Se adoptará la política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Se aplicarán los siguientes lineamientos:

- a) Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña.
- b) Proteger las PC's o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso cuando no se utilizan.
- c) Cumplir con los requerimientos y procedimientos de seguridad en áreas protegidas.
- d) Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
- e) Guardar y proteger la información sensible o crítica del Organismo (preferentemente en gabinete ignifugo bajo llave o código PIN) cuando no está en uso, especialmente cuando no hay personal en la oficina.
- f) Desconectar de la red / sistema / servicio las computadoras personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso (como por ejemplo la utilización de protectores de pantalla con contraseña). Los responsables de cada área mantendrán un registro de las contraseñas o copia de las llaves de seguridad utilizadas en el sector a su cargo. Tales elementos se encontrarán protegidos en sobre cerrado o caja de seguridad para impedir accesos no autorizados, debiendo dejarse constancia de todo acceso a las mismas, y de los motivos que llevaron a tal acción.
- g) Proteger los puntos de recepción y envío de correo postal y las máquinas de fax no atendidas.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 62 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- h) Bloquear las fotocopiadoras (o protegerlas de alguna manera del uso no autorizado) fuera del horario normal de trabajo.
- i) Retirar inmediatamente la información sensible o confidencial, una vez impresa.

12. Cláusula: Seguridad de las Operaciones

Responsabilidad

El RSI es responsable de definir procedimientos, documentar controles y supervisar su implementación, definir las medidas necesarias para permitir la segregación de los ambientes de desarrollo, prueba y producción. Asegurar el registro de las actividades realizadas por el personal, para permitir su posterior revisión.

El RPI es responsable de conocer, participar en la definición de los controles y su implementación. Definir junto con el RSI los requerimientos para el resguardo de la información por la cual es responsable. Junto con el Responsable del Área de Producción de la Subgerencia Operativa de Informática evaluar el posible impacto operativo de los cambios a los sistemas y equipamiento y verificar su correcta implementación. Realizar las copias de resguardo de información, y los sistemas, así como la realización de pruebas periódica de la restauración de los sistemas usando dichas copias. Definir e implementar procedimientos para la administración y eliminación segura de medios informáticos de almacenamiento, como cintas, discos e informes impresos, entre otros. Junto con el responsable de las áreas de infraestructura y soporte, Implementar la sincronización de los relojes en todos los sistemas y dispositivos del Organismo.

12.1. Categoría: Procedimientos y responsabilidades operativos

Objetivo de control


Garantizar la operación correcta y segura de las instalaciones de procesamiento de la información.

12.1.1. Procedimientos operativos documentados

Control

Se deben documentar los procedimientos operativos y deben estar disponibles para todos los usuarios que los necesiten.

Las especificaciones de los requisitos de control deben considerar los controles automáticos a incorporar a los sistemas de información, así como la necesidad

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 63 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

de controles manuales de apoyo. Se debe aplicar consideraciones similares al evaluar paquetes de software, desarrollados o comprados.

Los requisitos y controles de seguridad deben ser acordes al valor que el Organismo les asigne a los activos de información involucrados (ver también Seguridad de los recursos humanos 7), y el daño potencial a la gestión, en que podrían ser afectados por una falla o ausencia de seguridad.

Los requisitos de la seguridad de la información de los sistemas y procesos, deben ser integrados en etapas tempranas de los proyectos. Los controles introducidos en la etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación.

Si los productos son comprados, se debe seguir un proceso formal de pruebas y de adquisición. Los contratos con el proveedor deben especificar los requisitos de seguridad identificados. Cuando la funcionalidad de seguridad en un producto propuesto no satisfaga los requisitos especificados, se debe reconsiderar el riesgo que se introduce y los controles asociados en forma previa a la compra del producto. Cuando se provea de funcionalidad adicional y cause un riesgo de seguridad, puede ser necesario desactivar o que se revise la estructura de control propuesta para determinar si se puede tener ventajas de esa mejora de la funcionalidad.

12.1.2. Gestión del cambio

Control


Se deben controlar los cambios en el Organismo, los procesos, las instalaciones de procesamiento de información y los sistemas que afecten a la seguridad de la información.

Los sistemas operacionales y el software de aplicación deben estar sujetos a una estricta gestión de control de cambios.

En particular, se deben considerar los siguientes puntos:

- a) identificación y registro de cambios significativos;
- b) planificación y pruebas de cambios;
- c) evaluación de impactos potenciales, incluyendo los impactos de seguridad de tales cambios;
- d) procedimiento formal de aprobación para los cambios propuestos;
- e) comunicación del detalle de cambios a las personas correspondientes;
- f) procedimientos de “vuelta atrás”, incluyendo procedimientos y responsabilidades para la suspensión y recuperación de cambios no exitosos y de eventos imprevistos.

Debe estar establecida la gestión formal de las responsabilidades y los procedimientos para asegurar el control satisfactorio de todos los cambios del

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 64 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

equipamiento, software o procedimientos. Cuando se realicen cambios, se debe guardar un registro de auditoría que contenga toda la información relevante.

12.1.3. Gestión de la capacidad

Control

Se debe realizar seguimiento y ajustar el uso de recursos y se deben realizar las proyecciones de futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.

Para cada actividad nueva y en curso, se deben identificar los requisitos de capacidad. Se deben realizar ajustes y seguimiento de los sistemas cuando sea necesario, para mejorar la disponibilidad y eficiencia de los sistemas. Se deben establecer los controles de detección para indicar problemas con suficiente antelación. Se debe tener en cuenta los nuevos requisitos de la gestión y de los sistemas, y las tendencias corrientes y proyectadas en las capacidades de procesamiento de información del Organismo para las proyecciones de futuros requisitos de capacidad.

Se necesitará poner particular atención en cualquier recurso que demande mucho tiempo adquirir o alto costo, por lo que los administradores deben realizar un seguimiento y control de la utilización de los recursos clave del sistema. Ellos deben identificar tendencias en el uso, particularmente en relación con la aplicación de la gestión o con el uso de herramientas de los sistemas de información.

Los RPI deben utilizar esta información para identificar y evitar potenciales cuellos de botella y la dependencia del personal clave que podría significar una amenaza a la seguridad o para los servicios del sistema, y un plan de acción apropiados.


12.1.4. Separación de los entornos de desarrollo, pruebas y producción.

Control

Se deben separar los entornos de desarrollo, pruebas y producción para reducir los riesgos de accesos no autorizados o cambios en el entorno de producción.

Se debe disponer un nivel de separación entre los ambientes operacionales (producción), de pruebas, y de desarrollo, que sea necesario para prevenir los problemas operacionales, se encuentre identificado y se implementen los controles apropiados.

Se deben considerar los elementos siguientes:

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 65 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- a) que se definan y documenten las reglas para la transferencia de software del estado de desarrollo al estado operacional (Operativo-Producción);
- b) que el software de desarrollo y el software operacional corran en diferentes sistemas o procesos de computación y en diferentes dominios o directorios;
- c) que los compiladores, editores, y otras herramientas de desarrollo o utilidades de sistema no se accedan desde sistemas operacionales cuando no se requiera;
- d) que el ambiente de prueba del sistema emule el ambiente operacional del sistema tanto como sea posible;
- e) que los usuarios utilicen distintos perfiles de usuario para los sistemas operacionales y de prueba, los menús deben mostrar mensajes y leyendas de identificación apropiados para reducir el riesgo de error;
- f) que los datos sensibles no se copien al ambiente de prueba del sistema (ver 12.4.2).

12.2. Categoría: Protección contra código malicioso

Objetivo de control

Asegurar que la información y las instalaciones de procesamiento de información estén protegidas contra código malicioso.

12.2.1. Controles contra código malicioso


Control

Se deben implementar los controles de detección, prevención y recuperación para la protección contra software malicioso, combinados con la concientización apropiada de los usuarios.

La protección contra el código malicioso debe ser software especializado en detección y reparación de código malicioso, conciencia de la seguridad, y de sistemas de acceso y controles con la gestión de cambios apropiados.

Se debe considerar la siguiente guía:

- a) establecer una política formal que prohíba el uso de software no autorizado (ver 12.6.2);
- b) establecer una política formal para proteger contra los riesgos asociados con la obtención de archivos y software, ya sea desde o a través de redes externas, o por cualquier otro medio, indicando qué medidas de protección se deben tomar;
- c) Realizar revisiones periódicas del contenido de software y datos de los sistemas que sustentan procesos críticos del Organismo; se deben investigar formalmente la presencia de archivos no aprobados o cambios no autorizados


Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 66 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- d) instalación y actualización periódica del software de detección del código malicioso y software de reparación para escanear las computadoras y los medios como control preventivo, o como rutina básica; las verificaciones llevadas a cabo deben incluir:
 - 1) la verificación de cualquier archivo, tanto en medios electrónicos o medios ópticos, y los archivos recibidos a través de las redes, antes de ser usado, en búsqueda de código malicioso;
 - 2) la verificación de los adjuntos de correos electrónicos y las descargas en búsqueda de código malicioso antes de su uso; esta verificación debe llevarse a cabo en diferentes lugares, por ejemplo: en servidores de correo electrónico, computadoras de escritorio, y cuando se ingrese a la red del Organismo;
 - 3) la verificación de las páginas de Internet en búsqueda de código malicioso;
- e) definir procedimientos y las responsabilidades para trabajar con la protección contra código malicioso en los sistemas, entrenándose en su uso, informando y recuperándose frente a ataques de códigos maliciosos;
- f) preparar planes de continuidad de la gestión adecuados para la recuperación de ataques de código malicioso, incluyendo todos los datos necesarios y el software de copias de seguridad y los acuerdos de recuperación (ver 17);
- g) implementar procedimientos para recolectar información de forma regular, tal como la suscripción a listas de correo y/o la verificación de los sitios de Internet que brindan información acerca de nuevo código malicioso;
- h) Implementar procedimientos para verificar la información relacionada con código malicioso, y asegurar que los boletines de alerta sean exactos e informativos; los RPI son responsables de que se utilicen fuentes calificadas, por ejemplo: publicaciones acreditadas, sitios de Internet de confianza o proveedores que producen software de protección contra código malicioso, para diferenciar entre engaños y código maliciosos real; se debe tener un plan de concientización para todos el personal de los problemas de los virus falsos ("hoax") y de qué hacer al recibirlos.

12.3. Categoría: Resguardo

Objetivo de control

Proteger contra la pérdida de datos.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 67 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

12.3.1. Resguardo de la información

Control


Se deben hacer copias para el resguardo de la información, el software y los sistemas, y se las debe someter a pruebas periódicamente de acuerdo con la política acordada de resguardo.

Se deben disponer de instalaciones de resguardo adecuadas para asegurar que toda la información y el software esencial puedan ser recuperados luego de un desastre o una falla del medio.

Se deben considerar los siguientes puntos en el resguardo de la información:

- a) que se defina el nivel necesario de la información de resguardo;
- b) que se produzcan registros precisos y completos de las copias de resguardo y procesos de restauración documentados;
- c) que se refleje en los requisitos del Organismo la extensión (por ejemplo: resguardo completo o diferencial) y la frecuencia de los resguardos, los requisitos de seguridad de la información involucrados y la criticidad de la información para la continuidad operativa del Organismo;
- d) que las copias de resguardo se almacenen en una ubicación remota, a una distancia suficiente para escapar de cualquier daño producido por un desastre en el sitio principal;
- e) que se le otorgue a la información de resguardo un adecuado nivel de protección física y de ambiente (ver Norma 11) consistente con las normas aplicadas al sitio principal; los controles aplicados en el sitio principal deben extenderse para cubrir el sitio de resguardo;
- f) que se prueben los medios de resguardo regularmente para asegurar que se puede confiar en ellos en casos de emergencia, cuando sea necesario;
- g) que los procedimientos de resguardo se verifiquen y prueben regularmente para asegurar que son efectivos y que pueden ser completados dentro del tiempo asignado en los procedimientos operacionales para la recuperación;
- h) en situaciones donde la confidencialidad es de importancia, el resguardo debe estar protegido por medios de encriptación.

El procedimiento de resguardo para los sistemas individuales se debe probar regularmente para asegurar que cumple con los requisitos de los planes de continuidad de la gestión (ver Norma 17). Para los sistemas críticos, los acuerdos de resguardo deben cubrir toda la información de sistemas, aplicaciones y los datos necesarios para la reconstrucción del sistema completo en un evento de desastre.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 68 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

Se debe determinar el período de retención de la información esencial del organismo, así como también cualquier requisito para archivar copias que deben ser guardadas permanentemente (ver 18.1.3).

12.4. Categoría: Registro y seguimiento

Objetivo de control

Registrar eventos y generar evidencia.

12.4.1. Registro de eventos

Control

Se debe producir, conservar y revisar periódicamente los registros de eventos en los cuales se registren las actividades de los usuarios, las excepciones, los errores y los eventos de seguridad de la información.

Las auditorías de las sesiones deben incluir, cuando corresponda:

- a) identificación de los usuarios;
- b) fechas, tiempos, y detalles de los eventos principales, por ejemplo, inicio y cierre de sesión;
- c) la identidad de la computadora o la ubicación si es posible;
- d) registros de intentos de acceso al sistema exitosos y rechazados;
- e) registros de intentos de acceso a los datos u otro recurso, exitosos y rechazados;
- f) cambios en la configuración del sistema;
- g) uso de privilegios;
- h) uso de utilitarios y aplicaciones de sistemas;
- i) archivos accedidos y el tipo de acceso;
- j) direcciones de redes y protocolos;
- k) alarmas ejecutadas por el sistema de control de accesos;
- l) activación y desactivación de los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusos.


12.4.2. Protección de la información de los registros

Control

Las instalaciones de procesamiento de los registros y la información de registros se deben proteger contra manipulación y acceso no autorizados.

Los controles deben estar orientados a la protección contra cambios no autorizados y problemas operacionales con las instalaciones de registro de sesión, incluyendo:

- a) alteraciones de los tipos de mensajes que son grabados;
- b) que los archivos de sesión se editen o eliminen;

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 69 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- c) que la capacidad de almacenamiento del medio del archivo de sesión se exceda, resultando en la falla para registrar los eventos o sobrescribiendo eventos registrados en el pasado.

Algunos registros de auditoría pueden requerir ser archivados como parte de la política de retención de registros o a causa de requisitos de recolectar y retener evidencia (ver también 16.1.7).

12.4.3. Registro de administradores y operadores

Control

Se debe llevar registro de las actividades de los administradores y operadores del sistema, y se debe proteger y revisar periódicamente los registros.

Los registros deben incluir:

- a) fecha y hora en el cual ocurre un evento (éxito o falla);
- b) la información acerca del evento (por ejemplo, los archivos manipulados) o la fallas (por ejemplo, los errores ocurridos y las acciones correctivas tomadas);
- c) qué cuenta y qué administrador u operador estuvo involucrado;
- d) qué procesos fueron involucrados.

Se deben revisar periódicamente los registros del administrador del sistema y del operador de sistema.


12.4.4. Sincronización de los relojes

Control

Dentro del Organismo, se deben sincronizar los relojes de todos los sistemas pertinentes de procesamiento de información de acuerdo a una única fuente de tiempo de referencia.

Cuando un dispositivo informático o de comunicaciones tiene la capacidad de operar un reloj de tiempo real, se debe establecer este reloj según una norma acordada, por ejemplo: Tiempo Universal Coordinado (UTC por sus siglas en inglés) o normas de horario local. Como algunos relojes son conocidos por fluctuar con el tiempo, se debe tener un procedimiento que verifique y corrija cualquier variación significativa.

La interpretación correcta del formato de fecha/hora es importante para garantizar que la visualización de la fecha y hora refleja la fecha y hora actuales. Es conveniente que las especificaciones locales (por ejemplo, el horario de verano) se tengan en cuenta.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 70 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

12.5. Categoría: Control del software de producción

Objetivo de control

Asegurar la integridad de los sistemas de producción.

12.5.1. Instalación del software en los sistemas de producción


Control

Se deben implementar procedimientos para controlar la instalación de software en los sistemas de producción.

A fin de minimizar el riesgo de alteración de los sistemas operacionales, se deben tener en cuenta las siguientes directrices para controlar los cambios:

- a) que la actualización de software operacional, aplicaciones y de las bibliotecas de programas sólo la realicen administradores entrenados bajo autorización apropiada del RSI (ver 9.4.5);
- b) que los sistemas operacionales sólo guarden el código ejecutable aprobado, y no código en desarrollo o compiladores;
- c) que el software de aplicaciones y de sistema operativo se implementen luego de una prueba extensiva y exitosa; las pruebas deben incluir pruebas de uso, de seguridad, de efectos en otros sistemas y de cuan amigable es al usuario, y es conveniente que se lleven a cabo en sistemas separados (ver también 12.1.4); se debe asegurar que todas las bibliotecas correspondientes al programa fuente hayan sido actualizadas;
- d) que se use un sistema de control para mantener el control de todo el software implementado, así como de la documentación del sistema;
- e) que se establezca una estrategia de vuelta atrás antes que se implementen los cambios;
- f) que se mantenga un registro de auditoría de todas las actualizaciones de las bibliotecas de programas operacionales;
- g) que se retengan las versiones previas del software de aplicación como una medida de contingencia;
- h) que las versiones viejas del software se archiven, junto con toda la información requerida, los parámetros, los procedimientos, los detalles de configuración, y el software de soporte como así también que se retengan los datos en archivos.

Es conveniente que el software provisto por un vendedor, que es usado en sistemas operacionales se mantenga en un nivel en el que el proveedor les de soporte. A través de tiempo, los vendedores de software cesarán de dar soporte a las viejas versiones de software. El Organismo debe considerar los riesgos de depender de software que no tiene servicio de soporte.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 71 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

Cualquier decisión de actualizar una nueva versión debe tener en cuenta los requisitos de la actividad, y la seguridad de la versión, por ejemplo, la introducción de una nueva funcionalidad de seguridad o el número y severidad de los problemas de seguridad que afectan esta versión. Es conveniente que los parches de software sean aplicados cuando éstos ayuden a eliminar o reducir las debilidades de la seguridad (ver también 12.6.1).

Es conveniente que el acceso físico o lógico sólo se dé a los proveedores con fines de soporte, y con aprobación del RSI. Se deben seguir y controlar las actividades del proveedor.

El software puede depender de módulos y software provistos externamente, se deben seguir y controlar para evitar cambios no autorizados, que puedan introducir debilidades de seguridad.

12.6. Categoría: Gestión de las vulnerabilidades técnicas

Objetivo de control

Prevenir la explotación de las vulnerabilidades técnicas.

12.6.1. Control de las vulnerabilidades técnicas


Control

Se debe obtener, de manera oportuna, información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan, se debe evaluar la del Organismo a tales vulnerabilidades, y se debe tomar las medidas apropiadas para tratar los riesgos asociados.

Se realizará un inventario actualizado y completo de los activos (ver 8.1.1) es un prerequisite para una efectiva gestión de vulnerabilidades técnicas. La información específica necesaria para dar soporte a la gestión de las vulnerabilidades técnicas incluye al vendedor de software, números de versión, estado actual del desarrollo (por ejemplo, qué software está instalado en qué sistemas), y las personas del Organismo responsables por el software.

Se debe tomar una acción oportuna en respuesta a la identificación de las vulnerabilidades técnicas potenciales en forma apropiada. Es conveniente que se sigan las siguientes directrices para establecer un proceso de gestión efectivo de las vulnerabilidades técnicas:

- a) que el Organismo defina y establezca los roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas, incluyendo seguimiento de la vulnerabilidad, evaluación de los riesgos de la vulnerabilidad, parches, rastreo del activo, y cualquier responsabilidad de coordinación requerida;


Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 72 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- b) que se identifiquen por software y otras tecnologías, basadas en la lista de inventario de activos (ver 8.1.1) los recursos de información que serán usados para identificar las vulnerabilidades técnicas relevantes y para mantener la conciencia sobre ellas; es conveniente que estos recursos de información se actualicen en base a los cambios en el inventario, o cuando se encuentren otros recursos nuevos o útiles;
- c) que se defina una línea de tiempo para reaccionar ante las notificaciones de las vulnerabilidades técnicas potencialmente relevantes;
- d) una vez que se ha identificado una potencial vulnerabilidad técnica, que el Organismo identifique los riesgos asociados y las acciones a llevar a cabo; tales acciones pueden involucrar la introducción de un parche a los sistemas vulnerables y/o las aplicaciones de otros controles;
- e) dependiendo de la urgencia con la que se debe atender la vulnerabilidad técnica, que la acción tomada se lleve a cabo de acuerdo con los controles relacionados con la gestión de cambios (ver 12.1.2) o siguiendo los procedimientos de respuesta a incidentes de seguridad de la información (ver 16.1);
- f) sí hay un parche disponible, que se atiendan los riesgos asociados a la instalación del parche (se deben comparar los riesgos presentados por la vulnerabilidad contra los riesgos de la instalación del parche);
- g) que se prueben y evalúen los parches antes de instalarlos para garantizar que son efectivos y que no tienen como resultado efectos secundarios que no puedan ser tolerados; si no existe un parche disponible, es conveniente que se consideren otros controles, tales como:
 - 1) desactivación de los servicios o las capacidades relacionados con la vulnerabilidad;
 - 2) adaptación o adición de controles de acceso, por ejemplo, “firewalls” de las fronteras de las redes (ver 13.1.3);
 - 3) incremento del seguimiento para detectar o prevenir ataques;
 - 4) aumento de la conciencia acerca de las vulnerabilidades;
- h) se debe mantener un registro de auditoría para todos los procedimientos emprendidos;
- i) El proceso de gestión de las vulnerabilidades técnicas debe seguirse y evaluarse regularmente para garantizar su efectividad y eficiencia;
- j) Se deben atender primero los sistemas de alto riesgo.

12.6.2. Restricciones a la instalación de software

Control

Se deben establecer e implementar reglas que gobiernen la instalación de software por parte de los usuarios.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 73 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

El Organismo definirá y aplicará una política estricta sobre qué tipos de software pueden instalar los usuarios.

Deberá aplicarse el principio de privilegios mínimos. Si se les concede ciertos privilegios, los usuarios pueden tener la capacidad de instalar software. El Organismo deberá identificar qué tipos de instalaciones de software son las permitidas (por ejemplo, actualizaciones y parches de seguridad al software existente) y qué tipos de instalaciones se encuentran prohibidas (por ejemplo, software que es sólo para uso personal y software cuyo origen pueda ser potencialmente dañino, desconocido o sospechoso). Estos privilegios deberán concederse teniendo en cuenta las funciones de los usuarios afectados.

12.7. Categoría: Consideraciones para las auditorías de sistemas de información

Objetivo de control

Minimizar el impacto de las actividades de auditoría sobre los sistemas de producción.


12.7.1. Controles de la auditoría de sistemas de información

Control

Los requisitos y las actividades de auditoría que involucren la verificación de los sistemas de producción se deben planificar cuidadosamente y acordar a fin de minimizar las interrupciones de los procesos de gestión.

Se deben contemplar las directrices siguientes:

- a) que los requisitos de auditoría se acuerden con el área que corresponda;
- b) que se acuerde y controle el alcance de las verificaciones;
- c) que las verificaciones se encuentren limitadas a un acceso de sólo lectura, al software y a los datos;
- d) que cualquier acceso que no sea de sólo lectura solamente se permita a copias aisladas de archivos del sistema, las cuales es conveniente que se eliminen una vez finalizada la auditoría, o se le otorgue protección adecuada si existe una obligación de mantener dichos archivos como requisitos de documentación de auditoría;
- e) que se identifiquen claramente y se dispongan los recursos para llevar a cabo las verificaciones;
- f) que se identifiquen y acuerden los requisitos de procesamiento especial o adicional;
- g) que se sigan y controlen todos los accesos, y se lleve registro de ellos para producir un rastro de referencia; se debe considerar el uso de huellas de referencias de tiempo para los sistemas o datos críticos;

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 74 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- h) que se documenten todos los procedimientos, requisitos y responsabilidades;
- i) que las personas que lleven a cabo la auditoría sean independientes de las actividades a auditar.

13. Cláusula: Seguridad de las Comunicaciones

Responsabilidad

El CGS es responsable de identificar, revisar periódicamente y documentar los requisitos para que los acuerdos de confidencialidad reflejen las necesidades del Organismo respecto a la protección de su información.

El RSI es responsable de asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información que la soportan. Controlar el uso responsable de herramientas informáticas de comunicación, como el correo electrónico, mensajería instantánea, acceso a contenidos vía Internet, entre otras.

Junto con el responsable de las áreas de infraestructura definir e implementar una debida segregación de redes.

13.1. Categoría: Gestión de la seguridad de la red

Objetivo de control

Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información que la soportan.

13.1.1. Controles de red


Control

Se debe gestionar y controlar las redes para proteger la información en sistemas y aplicaciones.

Los administradores deben implementar controles para asegurar la seguridad de la información en las redes, y la protección de los servicios conectados contra acceso no autorizado.

En particular, se deben considerar los puntos siguientes:

- 1) que la responsabilidad operacional para las redes se encuentre separada de las operaciones de computadoras, según corresponda;
- 2) que se establezcan los procedimientos y responsabilidades para la gestión del equipamiento remoto, incluyendo los equipos en las áreas de usuarios;
- 3) que se establezcan controles especiales para salvaguardar la confidencialidad e integridad de los datos que pasan a través de redes

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 75 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

públicas, y para proteger los sistemas conectados; también pueden requerirse controles especiales para mantener la disponibilidad de los servicios de red y de las computadoras conectadas;

- 4) la aplicación de un método de identificación apropiado, así como de seguimiento para permitir que se lleve un registro de las acciones relevantes de seguridad;
- 5) que las actividades gerenciales se encuentren estrechamente coordinadas tanto para optimizar el servicio de red para el Organismo como para garantizar que los controles se aplican consistentemente a través de toda la infraestructura de procesamiento de información.

13.1.2. Seguridad de los servicios de red

Control

Se debe identificar e incluir en cualquier acuerdo de servicios de red los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, ya sean servicios provistos por el Organismo o terceras partes.

Se debe determinar y controlar regularmente la capacidad del proveedor de servicio de red para gestionar los servicios acordados en un modo seguro, y que se acuerde el derecho de auditarlo.

Se deben identificar los acuerdos de seguridad necesarios para servicios particulares, tales como características de seguridad, niveles de servicio y los requisitos de gestión. El Organismo debe asegurar que los proveedores de servicios de redes implementan estas medidas.


13.1.3. Segregación de redes

Control

Los grupos de servicios de información, los usuarios y los sistemas de información, se deben segregar en más de una red.

Un método para controlar la seguridad de redes amplias es dividir las en dominios lógicos de red separados, por ejemplo, dominios de red internos y dominios de red externos a una organización, cada uno protegido por un perímetro de seguridad definido. Se puede aplicar un conjunto graduado de controles en diferentes dominios de redes lógicas para separar aún más los ambientes de seguridad de la red, por ejemplo, sistemas públicamente accesibles, redes internas y activos críticos. Los dominios deben ser definidos en base a una evaluación de riesgos y a diferentes requisitos de seguridad dentro de cada dominio.

Tal perímetro de red puede ser implementado mediante la instalación de una puerta de enlace ("gateway") segura entre dos redes que serán interconectadas para controlar el acceso y el flujo de la información entre los dos dominios. Este

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 76 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

pasaje debe configurarse para filtrar el tráfico entre estos dominios y para bloquear el acceso no autorizado en concordancia con la política de control de acceso del Organismo (ver 9.1). Un ejemplo de este tipo de puerta de enlace es el que comúnmente se conoce como “firewall”. Otro método de dividir los dominios lógicos separados es la restricción al acceso de redes utilizando redes privadas virtuales para grupos de usuarios dentro del Organismo.

Las redes también pueden ser divididas usando funcionalidades de los dispositivos de red, por ejemplo, conmutación de IP (IP Switching). Los dominios separados pueden implementarse por el control del flujo de datos de red usando capacidades de conmutación (switching) y enrutamiento (routing), tales como listas de control de accesos.

El criterio para la subdivisión de redes en dominios debe basarse en la política de control de acceso y los requisitos de acceso, y también se tenga en cuenta el costo relativo y el impacto de desempeño de la incorporación de un adecuado enrutamiento o tecnología de puerta de enlace (gateway) de red (ver 13.1).

La subdivisión de redes debe basarse en el valor y la clasificación de la información almacenada o procesada en la red, niveles de confiabilidad, o lineamientos de la gestión, para reducir el impacto total de la interrupción de servicio.

Se debe considerar la separación de redes inalámbricas de las redes internas y privadas. Como los perímetros de redes inalámbricas no están bien definidos, se debe llevar a cabo una evaluación de riesgos en tales casos para identificar controles (por ejemplo, autenticación fuerte, métodos criptográficos, y selección de la frecuencia) para mantener la subdivisión de redes.

13.2. Categoría: Transferencia de información

Objetivo de control


Mantener la seguridad de la información transferida dentro del Organismo y con cualquier entidad externa.

13.2.1. Políticas y procedimientos de transferencia de información


Control

Se deben establecer políticas, procedimientos y controles formales para proteger la transferencia de información a través del uso de todo tipo de instalación de comunicaciones.

Los procedimientos y controles a seguir cuando se utilizan las instalaciones de comunicación electrónica para el intercambio de la información deben considerar los siguientes puntos:

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 77 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- a) procedimientos diseñados para proteger la información intercambiada de la interceptación, copia, modificación, mal direccionamiento y destrucción;
- b) procedimientos para la detección de y la protección contra el código malicioso que puede ser transmitido a través del uso de comunicaciones electrónicas;
- c) procedimientos para la protección de la información electrónica sensible comunicada que se encuentra en forma de adjunta;
- d) políticas o directrices que den lineamientos sobre el uso aceptable de las instalaciones de comunicación electrónicas;
- e) procedimientos para el uso de comunicaciones inalámbricas, teniendo en cuenta los riesgos particulares involucrados;
- f) responsabilidades del empleado, personal contratado y cualquier otro usuario de no comprometer al Organismo, por ejemplo, a través de la difamación, hostigamiento, suplantación de identidad, reenvío de cadenas de cartas, compras no autorizadas, etc.;
- g) uso de técnicas criptográficas, por ejemplo, para proteger la confidencialidad, integridad y la autenticidad de la información;
- h) directrices de retención y eliminación para toda la correspondencia del Organismo, incluyendo mensajes, en concordancia con las leyes y regulaciones correspondientes, locales y nacionales;
- i) no dejar la información crítica o sensible en las instalaciones de impresión, por ejemplo: copiadoras, impresoras, y equipos de fax, que pueden ser accedidos por personal no autorizado;
- j) establecer controles y restricciones asociadas a las instalaciones de reenvío de comunicación, por ejemplo: reenvío automático de correo electrónico a direcciones de mail externas;
- k) recordar al personal que deben tomar las precauciones adecuadas, por ejemplo: de no revelar información sensible para evitar que por casualidad se escuche o intercepte cuando se realiza una llamada telefónica por:
 - 1) gente en su cercanía inmediata, particularmente cuando se utiliza teléfonos móviles;
 - 2) intervenciones del cableado, y otras formas de indiscreciones a través del acceso físico al tubo del teléfono o a la línea telefónica, o usando dispositivos de búsqueda;
 - 3) gente al lado del receptor;
- l) no dejar mensajes que contengan información sensible en contestadores automáticos debido a que pueden ser reproducidos por personas no autorizadas; almacenadas en los sistemas comunes; o incorrectamente, como resultado de un error de discado;
- m) recordar al personal acerca de los problemas del uso de equipos de fax, como ser:
- n) el acceso no autorizado a la casilla de almacenamiento de mensajes para la recuperación;

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 78 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- o) la programación deliberada o accidental de equipos para enviar mensajes a números específicos;
- p) envío de documentos y mensajes al número equivocado por haber discado mal o por haber utilizado un número almacenado equivocado;
- q) recordar al personal que no se registren datos demográficos, tales como direcciones de correo electrónico u otra información personal, en cualquier software para evitar su recuperación para un uso no autorizado;
- r) recordar al personal que los modernos equipos de fax y las fotocopiadoras tienen memoria para guardar páginas en caso de falla de papel o de la transmisión, la cual será impresa una vez que la falla haya sido solucionada.

Además, se le debe recordar al personal que no mantengan conversaciones confidenciales en lugares públicos u oficinas abiertas, así como tampoco en lugares de reunión sin paredes a prueba de sonido.

Las instalaciones de intercambio de información deben cumplir con los requisitos legales correspondientes.


13.2.2. Acuerdos de transferencia de información

Control

Los acuerdos deben abordar la transferencia segura de la información de gestión entre el Organismo y las partes externas.

Los acuerdos de intercambio deben considerar las condiciones de seguridad siguientes:

- a) responsabilidades gerenciales para controlar y notificar la transmisión, envío y recepción;
- b) procedimientos para notificar al emisor de la transmisión, envío y recepción;
- c) procedimientos para asegurar la trazabilidad y el no repudio;
- d) normas técnicas mínimas para el empaquetado y la transmisión;
- e) acuerdos de fideicomiso;
- f) normas de identificación de los servicios de mensajería;
- g) las responsabilidades y obligaciones en caso de incidentes de seguridad de información, tales como pérdida de datos;
- h) uso de un sistema de rotulado acordado para la información sensible o crítica, que asegure que el significado de los rotulados se entienda inmediatamente y que la información se proteja adecuadamente;
- i) la propiedad y las responsabilidades por la protección de datos, *copyright*, cumplimiento de las licencias de software y consideraciones similares (ver Capítulo 18);

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 79 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- j) normas técnicas para el grabado y la lectura de la información y del software;
- k) cualquier control especial que pueda ser requerido para proteger artículos sensibles, como las claves criptográficas.

Deben establecerse y mantenerse políticas, procedimientos, y normas para proteger la información y medios físicos en tránsito y deben ser referenciados en tales acuerdos de intercambio.

El contenido de seguridad de cualquier acuerdo debe reflejar la sensibilidad de la información comercial involucrada.

13.2.3. Mensajería electrónica

Control

Se debe proteger apropiadamente la información involucrada en la mensajería instantánea.

Se define como obligatorio el uso de la cuenta de correo electrónico institucional a todos los agentes y funcionarios del organismo para toda comunicación vinculada con sus funciones.

Los mensajes electrónicos deben incluir las siguientes consideraciones de seguridad:


- a) protección de mensajes contra el acceso no autorizado, modificaciones o denegación de servicio;
- b) la correcta asignación de la dirección y el transporte del mensaje;
- c) confiabilidad y disponibilidad general del servicio;
- d) consideraciones legales, por ejemplo, requisitos de las firmas electrónicas;
- e) obtención de aprobación previa al uso de los servicios públicos externos tales como mensajería instantánea o archivos compartidos;
- f) niveles altos de controles de autenticación para los accesos desde las redes públicamente accesibles.

13.2.4. Acuerdos de confidencialidad

Control

Se deben identificar, revisar periódicamente y documentar los requisitos para que los acuerdos de confidencialidad reflejen las necesidades del Organismo respecto a la protección de su información.

Los acuerdos de confidencialidad o de no divulgación deben abarcar los requisitos de protección de la información confidencial usando términos legales aplicables. Para identificar los requisitos para los acuerdos de confidencialidad o de no divulgación, se deben considerar los siguientes elementos:

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 80 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- a) una definición de la información a ser protegida (por ejemplo: información confidencial);
- b) duración esperada de un acuerdo, incluyendo casos donde la confidencialidad podría mantenerse indefinidamente;
- c) acciones requeridas cuando un acuerdo finaliza;
- d) responsabilidades y acciones de las partes firmantes para evitar la divulgación no autorizada de la información (como ser el “need to know”);
- e) propiedad de la información, secretos comerciales y propiedad intelectual, y su relación con la protección de la información confidencial;
- f) el uso permitido de información confidencial, y los derechos de las partes firmantes para usar la información;
- g) el derecho para auditar y supervisar actividades que involucren información confidencial;
- h) procesos de notificación e informe de la divulgación no autorizada o de violaciones de la confidencialidad de la información;
- i) términos para que la información se devuelva o destruya al finalizar el acuerdo y
- j) acciones esperadas a llevarse a cabo en caso de incumplimiento de este acuerdo.

Basándose en los requisitos de seguridad de una organización, pueden llegar a ser necesarios otros elementos en los acuerdos de confidencialidad o de no divulgación.

Los acuerdos de confidencialidad y de no divulgación deben cumplir con todas las leyes y regulaciones aplicables para la jurisdicción en la cual se apliquen.


Los requisitos para los acuerdos de confidencialidad y no divulgación deben ser revisados periódicamente, así como también cuando ocurran cambios que influyan sobre dichos requisitos.

14. Cláusula: Adquisición, Desarrollo y Mantenimiento de los Sistemas

Responsabilidad

El CGS es responsable de verificar que la seguridad de la información sea una parte integral de los sistemas de información a lo largo de todo el ciclo de vida.

El RSI es responsable de asegurar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida del desarrollo de los sistemas de información. Definir procedimientos que brinden una debida protección de la información involucrada en las transacciones de los servicios de aplicaciones.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 81 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

El RPI de la Información es responsable de asegurar la protección de los datos utilizados para las pruebas. Implementar la debida protección de la información involucrada en las transacciones previniendo transmisiones incompletas, ruteo erróneo, alteración no autorizada de los mensajes, acceso indebido a opciones de sistemas, reescritura de scripts, cross site scripting, divulgación no autorizada, duplicación o repetición no autorizadas. Implementar un procedimiento de control de cambios. Junto con el Responsable del Área de desarrollo de sistemas de la Subgerencia Operativa de informática, incluirán los requisitos relacionados con la seguridad de la información dentro de los requisitos para los nuevos sistemas de información o las mejoras de los existentes.

14.1. Categoría: Requisitos de seguridad de los sistemas de información

Objetivo de control

Asegurar que la seguridad de la información sea una parte integral de los sistemas de información a lo largo de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proveen servicios a través de redes públicas.

14.1.1. Análisis y especificación de los requisitos de seguridad de la información


Control

Se debe incluir los requisitos relacionados con la seguridad de la información dentro de los requisitos para los nuevos sistemas de información o las mejoras de los existentes.

Se deben preparar procedimientos documentados para las actividades de los sistemas asociados con las instalaciones de procesamiento de información y de comunicación, tales como los procedimientos de inicio y apagado de la computadora, copias de resguardo, mantenimiento de los equipos, manejo de los medios, sala de computación y gestión de manejo de correo, y seguridad.

Los procedimientos operacionales deben especificar las instrucciones para la ejecución detallada de cada tarea, incluidas:

- a) procesamiento y manejo de información;
- b) copias de seguridad (ver 12.3);
- c) requisitos de tiempos, incluyendo interdependencias con otros sistemas, comienzos tempranos de inicio de tareas y finalización tardía de tareas;
- d) instrucciones para el manejo de errores u otras condiciones excepcionales que podrían surgir durante la ejecución de tareas, incluyendo restricciones en el uso de utilidades del sistema;
- e) contactos de soporte en caso de dificultades operativas o técnicas imprevistas;

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 82 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- f) instrucciones especiales para el manejo de salidas y medios, como el uso de papelería especial o la gestión de salida de resultados confidenciales, incluyendo procedimientos para la eliminación segura de las salidas de resultados de tareas fallidas (ver 8.3.2);
- g) procedimientos para el reinicio del sistema y procedimientos de recuperación para utilizar en caso de producirse fallas en el sistema;
- h) la gestión de hallazgos de auditoría e información de registros del sistema.

Los procedimientos operativos y los procedimientos documentados para las actividades del sistema deben ser tratados como documentos formales y los cambios sean autorizados por la Dirección. Cuando sea técnicamente viable, los sistemas de información se manejen consistentemente, usando los mismos procedimientos, herramientas y utilidades.


14.1.2. Aseguramiento de los servicios de aplicaciones sobre redes públicas

Control

Se deben incluir los requisitos relacionados con la seguridad de la información dentro de los requisitos para los nuevos sistemas de información o las mejoras de los existentes.

Las consideraciones de seguridad para el comercio electrónico deben incluir:

- a) el nivel de confidencialidad que requiere cada parte de las otras, exigiendo su identificación, por ejemplo, a través de autenticación;
- b) procesos de autorización asociados con quien puede definir los precios, emisión o firma de los principales documentos comerciales;
- c) asegurar que los socios comerciales están completamente informados de sus autorizaciones;
- d) determinar y cumplir requisitos de confidencialidad, integridad, prueba de envío y recepción de documentos importantes y el no-repudio de los contratos, por ejemplo, asociados con los procesos de licitación y contratos;
- e) el nivel de confianza requerido en la integridad de la lista de precios informada;
- f) la confidencialidad de cualquier dato o información sensible;
- g) la confidencialidad e integridad de cualquier transacción de orden, información de pago, detalles de direcciones de envío, y confirmación de recepciones;
- h) el grado de la verificación apropiada de la información de pago provista por un cliente;
- i) seleccionar la forma más apropiada de liquidación de pagos para prevenirse del fraude;
- j) el nivel de protección requerido para mantener la confidencialidad e integridad de la información de las órdenes;

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 83 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- k) evitar la pérdida o duplicación de la información de transacciones;
- l) responsabilidades asociadas con cualquier transacción fraudulenta;
- m) requisitos de seguros.

Muchas de las consideraciones antes mencionadas pueden ser alcanzadas por la aplicación de controles criptográficos teniendo en cuenta el cumplimiento de los requisitos legales (ver 10.1).

Los acuerdos de comercio electrónico entre los socios comerciales deben sustentarse en un acuerdo documentado, en el cual ambas partes cumplan los términos de comercio acordados, incluyendo los detalles de autorización. Pueden ser necesarios otros acuerdos con proveedores de servicios de información y de redes.

Se debe considerar la resistencia del servidor empleado para el comercio electrónico frente a un ataque, y las implicaciones de seguridad de cualquier interconexión de red requerida para la implementación de los servicios de comercio electrónico.


14.1.3. Protección de las transacciones de servicios de aplicaciones

Control

Se debe proteger la información involucrada en las transacciones de los servicios de aplicaciones para prevenir transmisiones incompletas, ruteo erróneo, alteración no autorizada de los mensajes, divulgación no autorizada, duplicación o repetición no autorizadas de los mensajes.

Las consideraciones de seguridad para las transacciones en línea deben incluir lo siguiente:

- a) el uso de firmas electrónicas para cada una de las partes involucradas en la transacción;
- b) todos los aspectos de la transacción, esto es para asegurar que:
 - 1) las credenciales de los usuarios de todas las partes se validen y verifiquen;
 - 2) la transacción se mantenga confidencial; y
 - 3) se mantenga la privacidad asociada con todas las partes involucradas;
- c) que los caminos de las comunicaciones entre las partes estén encriptados;
- d) que se utilicen protocolos seguros para la comunicación entre todas las partes involucradas;
- e) que se asegure que los almacenamientos de los detalles de las transacciones están ubicados fuera de cualquier ambiente públicamente accesible, por ejemplo, sobre una plataforma de almacenamiento existente en la Intranet organizacional, y no

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 84 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

mantenida y expuesta sobre un medio de almacenamiento directamente accesible desde Internet;

- f) que cuando se utilice autorización segura (por ejemplo, para los propósitos de emitir y mantener firmas digitales y/o certificados digitales) la seguridad esté integrada y embebida a través de todo el proceso de gestión de certificación / firma, de punta a punta.

14.2. Categoría: Seguridad en los procesos de desarrollo y de soporte

Objetivo de control

Asegurar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida del desarrollo de los sistemas de información.

14.2.1. Política de desarrollo seguro


Control

Se debe establecer reglas para el desarrollo de software y de sistemas y se deben aplicar a los desarrollos dentro del Organismo.

El desarrollo seguro es un requisito para construir un servicio, una arquitectura, un software y un sistema seguros. Dentro de una política de desarrollo seguro, debe incluirse los siguientes aspectos:

- a) La seguridad del entorno de desarrollo;
- b) La orientación sobre la seguridad en el ciclo de vida del desarrollo de software:
 1. Seguridad en la metodología de desarrollo de software;
 2. Fijar las directrices de codificación para cada lenguaje de programación utilizado;
- c) Los requisitos de seguridad en la etapa de diseño;
- d) Los controles de seguridad dentro de los hitos del proyecto;
- e) Los registros de seguridad;
- f) La seguridad en el control de la versión;
- g) El conocimiento de las aplicaciones de seguridad requerido;
- h) La capacidad de evitar, encontrar y fijar vulnerabilidades del desarrollador.

Las técnicas seguras de programación deberán utilizarse tanto para los nuevos desarrollos como en escenarios de reutilización de código donde las normas aplicables al desarrollo pueden no ser conocidas o no fueron consistentes con las mejoras prácticas actuales. Las normas de codificación segura deberán considerarse y cuando corresponda, utilizadas. Los desarrolladores deberán capacitarse en su uso y en las pruebas y en la revisión de código deberán verificar su uso.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 85 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

Si el desarrollo es subcontratado, el Organismo deberá obtener garantías de que las terceras partes cumplan con estas normas de desarrollo seguro (ver 14.2.7).

14.2.2. Procedimientos de control de cambios en los sistemas

Control

Se deben controlar los cambios a los sistemas dentro del ciclo de vida de desarrollo mediante el uso de procedimientos formales de control de cambios.


A fin de minimizar la alteración de los sistemas de información, es necesario que se documente y se ponga en vigor un proceso formal de control de cambios. La introducción de nuevos sistemas y de cambios grandes en los sistemas existentes sea seguida de un proceso formal de documentación, especificación, pruebas, control de calidad, e implementación gestionada.

Este proceso debe incluir una evaluación de riesgos, un análisis de los impactos de los cambios, y las especificaciones de los controles de seguridad necesarios. Estos procesos deben garantizar que no se hayan alterado los procedimientos de seguridad y control existentes, que los programadores de soporte sólo tengan acceso a aquellas partes del sistema necesarias para el desempeño de sus tareas, y que se obtenga un acuerdo y aprobación formales para cualquier cambio.

Siempre que resulte factible, los procedimientos de control de cambios operativos y de las aplicaciones deben encontrarse integrados (ver también 12.1.2).

Los procedimientos de cambio deben incluir:

- a) mantenimiento de un registro de los niveles de autorización acordados;
- b) garantía de que los cambios son propuestos por usuarios autorizados;
- c) controles de revisión y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios;
- d) identificación de todo el software, la información, las entidades de bases de datos y el hardware que requieran correcciones;
- e) aprobación formal para las propuestas detalladas antes de que comiencen las tareas;
- f) garantía de que los usuarios autorizados aceptan los cambios antes de su implementación;
- g) garantía de que el conjunto de documentación del sistema se encuentra actualizada cada vez que se completa un cambio y de que se archiva o elimina la documentación vieja;
- h) mantenimiento de un control de versiones para todas las actualizaciones de software;

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 86 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- i) mantenimiento de una huella de auditoría de todas las solicitudes de cambios;
- j) garantizar que la documentación operativa (ver 12.1.1) y los procedimientos de usuarios se modifiquen según las necesidades para que se mantenga adecuada;
- k) garantía de que la implementación de los cambios tenga lugar en el momento adecuado y no altere los procesos productivos involucrados.

14.2.3. Revisiones técnicas de las aplicaciones luego de cambios en la plataforma de producción

Control

Cuando se cambian los sistemas de producción, se debe revisar y probar las aplicaciones críticas de la gestión para asegurar que no se produzca un impacto adverso en las operaciones o en la seguridad del Organismo.

Este proceso debe cubrir:

- a) la revisión de procedimientos de integridad y control de aplicaciones para garantizar que éstos no hayan sido comprometidos por los cambios del sistema operativo;
- b) la garantía de que el plan y presupuesto de soporte anual contemple las revisiones y las pruebas del sistema como consecuencia del cambio en el sistema operativo;
- c) la garantía de que se notifiquen los cambios del sistema operativo en tiempo, para permitir que se lleven a cabo pruebas y revisiones apropiados antes de la implementación;
- d) la garantía de que se realicen los cambios apropiados a los planes de continuidad de la gestión (ver Norma 17).


14.2.4. Restricciones a los cambios en los paquetes de software

Control

Se deben desalentar las modificaciones en los paquetes de software, limitarlas a los cambios necesarios y controlar estrictamente todos los cambios.

En la medida de lo posible, y de lo viable, los paquetes de software suministrados por proveedores se utilicen sin modificaciones. Cuando sea necesario modificar un paquete de software, se deben considerar los siguientes puntos:

- a) el riesgo de que se comprometan los procesos de integridad y controles incorporados;
- b) si es conveniente la obtención del consentimiento del proveedor;

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 87 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- c) la posibilidad de obtener los cambios requeridos a través del proveedor en forma de actualizaciones normales de programas;
- d) el impacto que se produciría si el Organismo se hace responsable del mantenimiento futuro del software como resultado de los cambios.

Si los cambios se consideran necesarios, se debe retener el software original y se apliquen los cambios a una copia claramente identificada. Se implementará un proceso de gestión de actualización del software para garantizar que se instalen los parches aprobados y las actualizaciones de aplicaciones más actualizadas para todo el software autorizado. Todos los cambios deben ser probados y documentados completamente, de manera que puedan aplicarse nuevamente, de ser necesario, a futuras actualizaciones de software. En caso de ser necesario, las modificaciones deben ser probadas y validadas por un ente evaluador independiente.

14.2.5. Principios de seguridad en el desarrollo de sistemas


Control

Se deben establecer, documentar, mantener y aplicar los principios de seguridad para el desarrollo de sistemas seguros en la implementación de sistemas de información.

Los principios de la ingeniería de sistemas seguros de información basados en los principios de ingeniería de seguridad, deberán establecerse, documentarse y aplicarse a las actividades internas de ingeniería de sistemas de información. La seguridad debería diseñarse en todas las capas de arquitectura (negocios, datos, aplicaciones y tecnología) equilibrando la necesidad de seguridad de la información con la necesidad de la accesibilidad. Deberá analizarse la nueva tecnología para los riesgos de seguridad y el diseño debería revisarse contra patrones de ataque conocidos.

Estos principios y procedimientos de ingeniería establecidos deberán revisarse regularmente, para asegurar que están contribuyendo eficazmente a mejores normas de seguridad dentro del proceso de ingeniería. Estos también deberán revisarse periódicamente para asegurar que permanezcan actualizados en cuanto a la lucha contra las nuevas amenazas potenciales, y que sigan siendo aplicables a los avances en las tecnologías y soluciones a ser aplicadas.

Los principios establecidos de ingeniería de la seguridad deberán aplicarse, cuando corresponda, a los sistemas de información subcontratados a través de contratos, y de otros acuerdos vinculantes entre el Organismo y el proveedor contratado. El Organismo deberá confirmar que el rigor de los principios de ingeniería de seguridad de los proveedores es comparable con el propio.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 88 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

14.2.6. Entorno seguro de desarrollo

Control

El Organismo debe establecer y proteger apropiadamente los entornos seguros de desarrollo para los esfuerzos de desarrollo e integración que cubran todo el ciclo de vida de desarrollo de los sistemas.

El Organismo deberá evaluar los riesgos asociados con los esfuerzos de desarrollo del sistema individual y establecer ambientes de desarrollo seguro para esfuerzos de desarrollo específicos del sistema, considerando:

- a) Sensibilidad de los datos a ser procesados, almacenados y transmitidos por el sistema;
- b) Requisitos externos e internos aplicables, por ejemplo, de reglamentos o políticas;
- c) Los controles de seguridad ya implementados por el Organismo que apoyan el desarrollo del sistema;
- d) La confiabilidad del personal que trabaja en el ambiente (ver 7.1.1);
- e) El grado de contratación externa asociado con el desarrollo del sistema;
- f) La necesidad de separación entre diferentes ambientes de desarrollo;
- g) El control de acceso al ambiente de desarrollo;
- h) Seguimiento del cambio al ambiente y el código almacenado en el mismo;
- i) Los respaldos son almacenados en locaciones seguras fuera de las instalaciones;
- j) El control sobre el movimiento de los datos desde y hacia éste ambiente.

Una vez que el nivel de protección es determinado para un ambiente de desarrollo específico, el Organismo deberá documentar los procesos correspondientes de los procedimientos de desarrollo seguro y proporcionarlos a todas las personas que los necesiten.


14.2.7. Desarrollo provisto por terceras partes

Control

El Organismo debe supervisar y realizar el seguimiento de las actividades de desarrollo de los sistemas provistas por terceras partes.

Cuando se terceriza el desarrollo del software, se consideren los puntos siguientes:

- a) Acuerdos de licencias, propiedad de código y derechos de propiedad intelectual (ver 18.1.2).
- b) Certificación de la calidad y precisión del trabajo llevado a cabo;
- c) Acuerdos de custodia ("escrow") en caso de falla de la tercera parte;
- d) Derechos de acceso para auditar la calidad y precisión del trabajo realizado.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 89 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- e) Requisitos contractuales con respecto a la calidad y a la seguridad funcional del código.
- f) Realización de pruebas previas a la instalación, para detectar código troyano y malicioso.

14.2.8. Pruebas de seguridad de los sistemas

Control

Se deben realizar pruebas de las funcionalidades de seguridad durante el desarrollo.

Los sistemas nuevos y actualizados requieren pruebas exhaustivas y verificación durante los procesos de desarrollo, incluyendo la preparación de un programa detallado de actividades y los insumos de pruebas y los resultados esperados bajo una serie de condiciones. En cuanto a los desarrollos internos, tales pruebas deben realizarse inicialmente por parte del equipo de desarrollo. Las pruebas independientes de aceptación deberán realizarse (tanto para el desarrollo interno como para el subcontratado) para asegurar que el sistema funciona como se esperaba y solo como se esperaba (ver 14.1.1 y 14.1.2). El alcance de las pruebas deberá ser proporcional a la importancia y naturaleza del sistema.


14.2.9. Pruebas de aceptación de los sistemas

Control

Se deben establecer criterios y programas de pruebas de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas.

Los Directivos deben garantizar que los requisitos y criterios de aceptación de nuevos sistemas estén claramente definidos, acordados, documentados y probados. Los nuevos sistemas de información, las actualizaciones, y las nuevas versiones solamente se deben migrar a producción después de que se obtenga la aceptación formal. Antes de que se realice la aceptación formal se deben considerar siguientes los puntos:

- a) requisitos de capacidad y desempeño de las computadoras;
- b) recuperación ante errores y procedimientos de reinicio, y planes de contingencia;
- c) preparación y prueba de procedimientos operativos de rutina según normas definidas;
- d) conjunto acordado de controles de seguridad establecidos;
- e) procedimientos manuales eficaces;
- f) acuerdos para la continuidad de la gestión (ver 17.1);
- g) evidencia de que la instalación del nuevo sistema no afectará negativamente los sistemas existentes, especialmente en los períodos pico de procesamiento, como por ejemplo durante los últimos días del mes;

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 90 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- h) evidencia de que se ha tomado en consideración al efecto que tiene el nuevo sistema en la seguridad global del Organismo;
- i) entrenamiento en la operación o uso de nuevos sistemas;
- j) facilidad de uso, cómo esto afecta el desempeño del usuario y cómo evita el error humano.

Para los desarrollos nuevos, se deben consultar las funciones y usuarios de operaciones en todas las etapas del proceso de desarrollo para garantizar la eficiencia operacional del diseño del sistema propuesto. Se deben llevar a cabo pruebas apropiadas para confirmar que todos los criterios de aceptación fueron totalmente satisfechos.

La aceptación puede incluir un proceso de certificación y acreditación formal para verificar que se han alcanzado adecuadamente los requisitos de seguridad.

14.3. Categoría: Datos de prueba

Objetivo de control

Asegurar la protección de los datos utilizados para las pruebas.


14.3.1. Protección de los datos de prueba

Control

Los datos de prueba se deben seleccionar cuidadosamente, proteger y controlar.

Deberá evitarse el uso de los datos operativos que contengan información personal o cualquier otra información confidencial para fines de prueba. Si se utiliza información personal o cualquier otra información sensible para hacer pruebas, todos los detalles y el contenido sensible deberá eliminarse o modificarse (ver ISO/IEC 29101).

- a) Las directrices siguientes deberán aplicarse para proteger datos de producción cuando son utilizados para hacer pruebas:
- b) Los procedimientos de control de acceso, que se aplican a sistemas de aplicaciones en producción, deberán aplicarse también a los sistemas de prueba de aplicaciones;
- c) Deberá autorizarse por separado, cada vez que se copie la información de producción a un ambiente de prueba;
- d) Deberá borrarse la información de producción de un sistema de prueba de aplicación inmediatamente después de que las pruebas son completadas;
- e) Deberá registrarse la copia y el empleo de información de producción para proporcionar una pista de auditoría.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 91 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

15. Cláusula: Relaciones con los Proveedores

Responsabilidad

El RSI, junto con los RPI, debe definir en función a la criticidad de la información, los requerimientos de protección en lo referente al acceso de la información de los proveedores durante todo su ciclo de vida con el Organismo. Asimismo, todo responsable de las áreas legales, compras o que gestionen los contratos con proveedores, deben garantizar que en los mismos se definan y se acuerden los niveles de seguridad establecidos por el Organismo.

15.1. Categoría: Seguridad de la información en las relaciones con los proveedores

Objetivo de control

Asegurar la protección de los activos del Organismo a los cuales tienen acceso los proveedores.

15.1.1. Política de seguridad de la información para las relaciones con los proveedores


Control

Se deben acordar con el proveedor y documentar los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso del proveedor a los activos del Organismo.

Se debe identificar e imponer controles de seguridad de la información para abordar específicamente el acceso de los proveedores a la información del Organismo.

Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de equipamiento de Trabajo del Organismo, contemplarán los siguientes aspectos:

- a) la identificación y la documentación de los tipos de proveedores, es decir, los servicios de TI, las utilidades de logística, los servicios financieros, los componentes de la infraestructura de TI y a quiénes el Organismo autorizará acceder a su información;
- b) un proceso estandarizado y el ciclo de vida para la gestión de relaciones con los proveedores;
- c) la definición de los tipos de acceso a la información que se les permitirá a los distintos tipos de proveedores y el monitoreo y control del acceso;
- d) requisitos de seguridad de la información mínimos para cada tipo de información y tipo de acceso para servir de base para los acuerdos

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 92 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		


- individuales con los proveedores en base a las necesidades del Organismo, los requisitos y su perfil de riesgo;
- e) procesos y procedimientos para monitorear la adherencia a los requisitos de seguridad de información establecidos para cada tipo de proveedor y tipo de acceso, incluida la revisión de terceros y la validación de productos;
 - f) controles de precisión y nivel de detalles para garantizar la integridad de la información o el procesamiento de información que entrega cualquiera de las partes;
 - g) tipos de obligaciones aplicables a los proveedores para proteger la información;
 - h) manejo de incidentes y contingencias asociadas con el acceso a los proveedores, incluidas las responsabilidades del Organismo y los proveedores;
 - i) resiliencia y, en caso de ser necesario, disposiciones de recuperación y contingencia para garantizar la disponibilidad de la información o el procesamiento de información proporcionado por cualquiera de las partes;
 - j) capacitación de concientización para el personal del Organismo involucrado en las adquisiciones sobre políticas, procesos y procedimientos correspondientes;
 - k) capacitación de concientización para el personal del Organismo que interactúa con el personal de los proveedores en cuanto a las reglas adecuadas sobre el compromiso y el comportamiento en base al tipo de proveedor y el nivel de acceso del proveedor a los sistemas y la información del Organismo;
 - l) que las condiciones sobre los controles y requisitos de seguridad de la información se documentarán en un acuerdo firmado por ambas partes;
 - m) gestión de las transiciones necesarias de información, instalaciones de procesamiento de información y cualquier otra cosa que se deba mover y, garantizando que se mantiene la seguridad de la información a través de todo el período de transición.

15.1.2. Tratamiento de la Seguridad en los acuerdos con los proveedores

Control

Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información del Organismo.


Se deben establecer y documentar acuerdos con los proveedores para garantizar que no existen malos entendidos entre el Organismo y el proveedor

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 93 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

en cuanto a las obligaciones de ambas partes para cumplir con los requisitos de seguridad de la información pertinentes.

A continuación, se definen los términos para incluir en los acuerdos a fin de y poder satisfacer los requisitos de seguridad de la información identificados:

- a) descripción de la información que se debe proporcionar o a la que se debe acceder y los métodos para proporcionar o acceder a la información;
- b) clasificación de la información de acuerdo al esquema de clasificación del Organismo; y si es necesario también realizar el mapeo entre el esquema propio del Organismo y el esquema de clasificación del proveedor;
- c) requisitos legales y normativos, incluida la protección de datos personales, los derechos de propiedad intelectual y los derechos de autor y una descripción sobre cómo se garantizará que se cumplen;
- d) obligación de cada parte contractual para implementar un conjunto de controles acordados incluido el control de acceso, la revisión de desempeño, el monitoreo, los informes y la auditoría;
- e) reglas de uso aceptable de la información, incluido el uso inaceptable si es necesario;
- f) una lista explícita del personal autorizado para acceder o recibir la información o los procedimientos o condiciones del Organismo para su autorización y el retiro de la autorización, para el acceso o la recepción de la información del Organismo al personal del proveedor;
- g) políticas de seguridad de la información pertinentes al contrato específico;
- h) requisitos y procedimientos de la administración de incidentes (en especial la notificación y la colaboración durante la remediación de incidentes);
- i) requisitos de capacitación y concientización para procedimientos específicos y requisitos de seguridad de la información, es decir, para la respuesta ante incidentes y procedimientos de autorización;
- j) normativas pertinentes para la subcontratación, incluidos los controles que se deben implementar;
- k) socios de acuerdos pertinentes, incluida una persona de contacto para los asuntos de seguridad de la información;
- l) requisitos de selección, si existe alguno, del personal del proveedor para realizar los procedimientos de selección y notificación si no se ha completado la selección o si los resultados son motivo de dudas o inquietudes;
- m) derecho a auditar los procesos y los controles del proveedor relacionados al acuerdo;
- n) procesos de resolución de defectos y resolución de conflictos;
- o) obligación del proveedor a entregar periódicamente un informe independiente sobre la efectividad de los controles y un acuerdo

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 94 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

sobre la corrección oportuna de los asuntos pertinentes indicados en el informe;

- p) obligaciones del proveedor de cumplir con los requisitos de seguridad del Organismo.


15.1.3. Cadena de suministro de las tecnologías de la información y las comunicaciones

Control

Los acuerdos con los proveedores deben incluir requisitos para tratar los riesgos a la seguridad de la información asociada a la cadena de suministro de servicios y productos de las tecnologías de la información y las comunicaciones.

Se deben incluir los siguientes temas en los acuerdos con el proveedor sobre la seguridad de la cadena de suministro:

- a) definir los requisitos de seguridad de la información que se aplicarán a la adquisición de tecnologías, productos o servicios de tecnología de la información y comunicación además de los requisitos de seguridad de la información para las relaciones con el proveedor;
- b) para los servicios de tecnología de la información y las comunicaciones, se requiere que los proveedores propaguen los requisitos de seguridad de la información del Organismo en toda la cadena de suministro, si los proveedores realizan subcontrataciones de partes de la información o de servicios de tecnología de comunicación proporcionados al Organismo;
- c) para la información y los productos de tecnología de la comunicación, se requiere que los proveedores propaguen las prácticas de seguridad correspondientes a través de toda la cadena de suministro, si estos productos incluyen componentes comprados a otros proveedores;
- d) implementación de un proceso de monitoreo y métodos aceptables para validar que los productos y servicios de tecnología de la información y la comunicación se adhieren a los requisitos de seguridad establecidos;
- e) implementación de un proceso para identificar los componentes de los productos o servicios que son fundamentales para mantener la funcionalidad y que, por lo tanto, requiere una mayor atención y escrutinio cuando son construidos fuera del Organismo, especialmente si el proveedor del nivel superior subcontrata aspectos de los componentes de productos o servicios a otros proveedores;
- f) obtención de una garantía de que los componentes críticos y su origen se pueden rastrear en toda la cadena de suministros;
- g) obtener la garantía de que los productos de tecnología de la información y la comunicación entregados funcionan según lo esperado sin ninguna función inesperada o no deseada;

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 95 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- h) definición de las reglas para compartir la información en cuanto a la cadena de suministro y cualquier posible problema y compromiso entre el Organismo y los proveedores;
- i) implementación de procesos específicos para la gestión de la información y el ciclo de vida de los componentes de tecnología de la comunicación junto con la disponibilidad y los riesgos de seguridad asociados. Esto incluye la gestión de riesgos de los componentes que ya no están disponibles debido a que los proveedores ya no están o a que ya no proporcionan estos componentes debido a los avances tecnológicos.

15.2. Categoría: Gestión de la entrega de servicios prestados por los proveedores

Objetivo de control

Mantener un nivel acordado de seguridad de la información y de prestación de servicio alineados con los acuerdos con los proveedores.

15.2.1. Seguimiento y revisión de los servicios prestados por los proveedores


Control

Las organizaciones deben seguir, revisar y auditar periódicamente la entrega de los servicios prestados por los proveedores.

Se llevará a cabo el seguimiento, control y revisión de los servicios de las terceras partes asegurando que se encuentran adheridos a los términos de seguridad de la información y las condiciones definidas en los acuerdos, y que los incidentes y los problemas de la seguridad de la información son manejados correctamente.

El Organismo mantendrá control suficiente y visión general de todos los aspectos de seguridad para la información sensible o crítica, o de las instalaciones de procesamiento de información accedidas, procesadas o gestionadas por una tercera parte.

La responsabilidad de gestionar la relación con proveedores deberá asignarse a un individuo o a un equipo designado de gestión del servicio. Además, el Organismo deberá asegurarse de que los proveedores asignen responsabilidades de verificación para evaluar la conformidad y hacer cumplir los requisitos de los acuerdos. Los recursos técnicos y las habilidades técnicas deberán estar disponibles para supervisar que los requisitos del acuerdo, en particular los requisitos de seguridad de la información, se estén cumpliendo. Deberán tomarse las acciones adecuadas cuando se observen deficiencias en la entrega del servicio.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 96 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

Esto implica generar una relación y un proceso de gestión del servicio entre el Organismo y el proveedor para:

- a) supervisar niveles de desempeño del servicio para comprobar adherencia a los acuerdos;
- b) revisar los informes del servicio producidos por los proveedores y realizar reuniones de evaluación según los requisitos de los acuerdos;
- c) realizar auditorías de proveedores, conjuntamente con la revisión de los informes de los auditores independientes, si se encuentran disponibles, y seguimiento de los problemas identificados;
- d) entregar información sobre incidentes de la seguridad de la información y revisión de esta información según los requisitos de los acuerdos y las pautas y procedimientos de soporte;
- e) revisar pistas de auditorías confeccionadas por los proveedores y registros de los incidentes de seguridad, de los problemas operacionales, de las fallas, del rastreo de fallas y de interrupciones relacionadas con el servicio entregado;
- f) resolver y gestionar los problemas identificados;
- g) revisar los aspectos de seguridad de la información de las relaciones del proveedor con sus propios proveedores;
- h) asegurarse de que el proveedor mantiene la suficiente capacidad de servicio junto con los planes realizables diseñados para asegurar que los niveles de continuidad de servicio acordados se mantienen después de fallas en el servicio o desastres importantes.


El Organismo deberá mantener suficiente control y visibilidad en todos los aspectos de la seguridad de la información sensible o crítica, o de las instalaciones de procesamiento de la información accedida, procesadas o gestionadas por un proveedor. El Organismo deberá mantener la visibilidad sobre actividades de seguridad, tales como gestión del cambio, identificación de las vulnerabilidades, y reportes de incidentes y respuestas de la seguridad de la información mediante un proceso claramente definido.

15.2.2. Gestión de cambios en los servicios prestados por los proveedores

Control

Los cambios en la prestación de los servicios por parte de proveedores, incluyendo el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, se deben gestionar, teniendo en cuenta la criticidad de la información, sistemas y procesos de gestión involucrados y la reevaluación de los riesgos.

El proceso de gestión del cambio de un servicio de tercera parte debe considerar los siguientes aspectos:

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 97 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- a) cambios en los acuerdos con proveedores;
- b) cambios realizados por el Organismo para implementar:
 - 1) mejoras a los servicios actuales ofrecidos;
 - 2) desarrollo de nuevos sistemas y aplicaciones;
 - 3) modificaciones o actualizaciones de las políticas y de los procedimientos del Organismo;
 - 4) controles nuevos o modificados para resolver incidentes de la seguridad de la información y para manejar la seguridad.
- c) cambios en servicios de los proveedores para implementar:
 - 1) cambios y mejoras en las redes;
 - 2) uso de nuevas tecnologías;
 - 3) adopción de nuevos productos o versiones/lanzamientos;
 - 4) nuevas herramientas y ambientes de desarrollo;
 - 5) cambios a la localización física de las instalaciones del servicio;
 - 6) cambio de proveedores;
 - 7) subcontratación de otro proveedor.

16. Cláusula: Gestión de los Incidentes de Seguridad de la Información

Responsabilidad

El RSI será responsable de implementar los medios y canales necesarios, manejar los reportes de incidentes y anomalías de los sistemas. Asimismo, tomará conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

El RSI tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados, así como su comunicación al CGS y a los RPI.


El RSI tiene la responsabilidad de comunicar fehacientemente los procedimientos de Gestión de Incidentes a los empleados y contratados al inicio de la relación laboral.

Los usuarios de servicios de información, al momento de tomar conocimiento directo o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar formalmente las mismas al RSI.

16.1. Categoría: Gestión de los incidentes de seguridad de la información y mejoras

Objetivo de control

Asegurar un enfoque coherente y eficaz para la gestión de los incidentes de seguridad de la información, incluyendo la comunicación de los eventos y las vulnerabilidades de la seguridad.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 98 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		


16.1.1. Responsabilidades y Procedimientos

Control

Se deben establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

Se deben considerar los siguientes ítems:

- a) Contemplar y definir todos los tipos probables de incidentes relativos a seguridad, incluyendo como mínimo:
 - 1) Fallas operativas.
 - 2) Código malicioso.
 - 3) Intrusiones.
 - 4) Fraude informático.
 - 5) Error humano.
 - 6) Catástrofes naturales.
- b) Comunicar formalmente los incidentes a través de autoridades o canales apropiados tan pronto como sea posible.
- c) Contemplar los siguientes puntos en los procedimientos para los planes de contingencia normales (diseñados para recuperar sistemas y servicios tan pronto como sea posible):
 - 1) Definición de las primeras medidas a implementar.
 - 2) Análisis e identificación de la causa del incidente.
 - 3) Planificación e implementación de soluciones para evitar la repetición del mismo, si fuera necesario.
 - 4) Comunicación formal con las personas afectadas o involucradas con la recuperación del incidente.
 - 5) Notificación de la acción a la autoridad y/u Organismos pertinentes.
- d) Registrar pistas de auditoría y evidencia similar para:
 - 1) Análisis de problemas internos.
 - 2) Uso como evidencia en relación con una probable violación contractual o infracción normativa, o en marco de un proceso judicial.
- e) Implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema, garantizando:
 - 1) Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado.
 - 2) Documentación de todas las acciones de emergencia emprendidas en forma detallada.
 - 3) Comunicación de las acciones de emergencia al titular de la Unidad Organizativa y revisión de su cumplimiento.
 - 4) Constatación de la integridad de los controles y sistemas del Organismo en un plazo mínimo.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 99 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

En los casos en los que se considere necesario, se solicitará la participación de la Gerencia Operativa de Asuntos Legales en el tratamiento de incidentes de seguridad ocurridos.

Los incidentes de seguridad de la información pueden superar los límites del Organismo y los nacionales. Para responder a tales incidentes existe una necesidad en aumento de coordinar respuesta y compartir la información sobre estos incidentes con organizaciones externas como sea apropiado.

16.1.2. Presentación de informes sobre los eventos de seguridad de la información

Control

Los eventos de seguridad de la información se deben informar a través de canales de gestión apropiados, tan pronto como sea posible.

Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes.

Dicho procedimiento debe contemplar que, ante la detección de un supuesto incidente o violación de la seguridad, el RSI sea informado tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo.

Asimismo, mantendrá al CGS al tanto de la ocurrencia de incidentes de seguridad.


Los desperfectos u otros comportamientos anómalos del sistema pueden ser un indicador de un ataque a la seguridad o de una violación real a la seguridad y, por lo tanto, deberá siempre reportarse como un evento de seguridad de la información.

Todos los empleados y el personal contratado deberán ser advertidos de su responsabilidad de reportar cualquier evento de seguridad de la información lo más rápidamente posible. Deberán también conocer el procedimiento para reportar los eventos de seguridad de la información y el punto de contacto al que los eventos deberán reportar.

16.1.3. Presentación de informes sobre las vulnerabilidades de seguridad de la información

Control

Se debe requerir que los empleados y el personal contratado que utilicen los sistemas y servicios de información del Organismo informen cualquier vulnerabilidad de seguridad de la información observada o sospechada en sistemas o servicios.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 100 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

Los usuarios de servicios de información, al momento de tomar conocimiento directo o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar normalmente las mismas al RSI y/o RPI.

16.1.4. Evaluación y decisión sobre los eventos de seguridad de la información

Control

Se deben evaluar los eventos de seguridad de la información y decidir si se los debe clasificar como incidentes de seguridad de la información.

El punto de contacto deberá evaluar cada evento de seguridad de la información utilizando la escala acordada de clasificación de eventos e incidentes de seguridad de la información y decidir si el evento deberá ser clasificado como un incidente de seguridad de la información.

La clasificación y la priorización de incidentes pueden ayudar a identificar el impacto y el alcance de un incidente.

Los resultados de la evaluación y la decisión deberán registrarse en detalle con el fin de futura referencia y verificación.

16.1.5. Respuesta a los incidentes de seguridad de la información


Control

Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.

Los incidentes de seguridad de la información deberán responderse por un punto de contacto designado y otras personas relevantes del Organismo o partes externas.

La respuesta deberá incluir lo siguiente:

- a) la recopilación de evidencia tan pronto como sea posible después de la ocurrencia;
- b) la realización de análisis forenses de seguridad de la información, según corresponda
- c) escalamiento, según corresponda;
- d) garantizar que todas las actividades de respuesta involucradas son registradas adecuadamente para su posterior análisis;
- e) comunicar la existencia del incidente de seguridad de la información o los datos relevantes del mismo a otros clientes u organizaciones internas y externas con una necesidad de conocer;
- f) tratar las debilidades de seguridad de la información encontradas para causar o contribuir al incidente;

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 101 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- g) una vez que el incidente ha sido tratado con éxito, cerrarlo y grabarlo formalmente.

Deberá realizarse un análisis post-incidente, si corresponde, para identificar el origen del incidente.

De esta manera, se alcanza el primer objetivo de la respuesta a incidentes que es reanudar el "nivel de seguridad normal" y luego iniciar la recuperación necesaria.

16.1.6. Aprendizaje a partir de los incidentes de seguridad de la información

Control

Se debe utilizar el conocimiento obtenido del análisis y resolución de los incidentes de seguridad de la información para reducir la probabilidad o el impacto de futuros incidentes.

Se definirá un proceso que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información se utilizará para identificar aquellos que sean recurrentes o de alto impacto. Esto será evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

16.1.7. Recolección de la evidencia

Control


El Organismo debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de la información que se pueda utilizar como evidencia.

El Organismo debe verificar a intervalos regulares los controles de la continuidad de la seguridad de la información, establecido e implementados, para asegurar que sean válidos y eficaces durante situaciones adversas.

Deberán desarrollarse y seguirse procedimientos internos al tratar con evidencia para los propósitos de acción disciplinaria y legal.

Estos procedimientos de evidencia deberán proporcionar procesos de identificación, recolección, adquisición y conservación de evidencia de acuerdo con los diferentes tipos de medios, dispositivos y estado de los dispositivos, por ejemplo, encendido o apagado. Los procedimientos deberán tener en cuenta:

- a) la cadena de custodia;
- b) la seguridad de la evidencia;
- c) la seguridad del personal;
- d) las funciones y responsabilidades del personal involucrado;
- e) la competencia del personal;

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 102 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- f) la documentación;
- g) la reunión informativa.

Cuando se disponga, deberá buscarse la certificación u otros medios pertinentes de la calificación del personal y las herramientas, con el fin de fortalecer el valor de la evidencia preservada.

La evidencia forense puede trascender los límites organizacionales o jurisdiccionales. En tales casos, deberá asegurarse que el Organismo tenga derecho a recopilar la información requerida como evidencia forense. Deberán considerarse los requisitos de las distintas jurisdicciones para maximizar las posibilidades de admisión en todas las jurisdicciones pertinentes.

La identificación es el proceso que implica la búsqueda, el reconocimiento y la documentación de las posibles evidencias. La recolección es el proceso de reunir los elementos físicos que podrían contener evidencia potencial. La adquisición es el proceso de crear una copia de los datos dentro de un conjunto definido. La preservación es el proceso de mantener y salvaguardar la integridad y el estado original de la evidencia potencial.

Cuando se detecta un evento de seguridad de la información por primera vez, puede que no sea obvio si el evento va a resultar o no en una acción judicial. Por lo tanto, existe el peligro de que las evidencias necesarias sean destruidas intencionalmente o accidentalmente antes de que se dé cuenta de la gravedad del incidente.

17. Cláusula: Aspectos de Seguridad de la Información en la Gestión de la Continuidad de la gestión


Responsabilidad

El RSI participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia.

Los RPI y el RSI identificarán las amenazas con el fin de desarrollar un plan estratégico de contingencia para garantizar la continuidad de las actividades del Organismo.

Los Responsables de Procesos revisarán periódicamente los planes bajo su incumbencia, como así también identificar cambios en las disposiciones relativas a las actividades del Organismo aún no reflejadas en los planes de continuidad.

Los Administradores de cada plan verificarán el cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 103 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

El RSI en conjunto con el CGS tendrán a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información del Organismo frente a interrupciones imprevistas.

17.1. Categoría: Continuidad de la seguridad de la información

Objetivo de control

Incorporar la continuidad de la seguridad de la información en los sistemas de continuidad de gestión del Organismo.

17.1.1. Planificación de la continuidad de la seguridad de la información

Control


El Organismo debe determinar sus requisitos de seguridad de la información y de la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o un desastre.

Proceso de Administración de la continuidad del Organismo

El RSI, será el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de las actividades del Organismo.

Estos tendrán a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información del Organismo frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

- a) Identificar y priorizar los procesos críticos de las actividades del Organismo.
- b) Asegurar que todos los integrantes del Organismo comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad del Organismo.
- c) Elaborar y documentar una estrategia de continuidad de las actividades del Organismo consecuente con los objetivos y prioridades acordados.
- d) Proponer planes de continuidad de las actividades del Organismo de conformidad con la estrategia de continuidad acordada.
- e) Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
- f) Coordinar actualizaciones periódicas de los planes y procesos implementados.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 104 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- g) Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades del Organismo.
- h) Proponer las modificaciones a los planes de contingencia.

Continuidad de las Actividades y Análisis de los impactos

Con el fin de establecer un Plan de Continuidad de las Actividades del Organismo se deben contemplar los siguientes puntos:

- a) Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades, por ejemplo, fallas en el equipamiento, comisión de ilícitos, interrupción del suministro de energía eléctrica, inundación, incendio, desastres naturales, destrucción edilicia, atentados, etc.
- b) Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación. Dicha evaluación debe identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación.
- c) Identificar los controles preventivos, como por ejemplo sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de back up, los registros no electrónicos vitales, etc.

Esta actividad será llevada a cabo con la activa participación de los Responsables de los procesos y recursos de información de que se trate y el RSI, considerando todos los procesos de las actividades del Organismo y no limitándose a las instalaciones de procesamiento de la información.


Según los resultados de la evaluación de esta actividad, se desarrollará un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades del Organismo. Una vez que se ha creado este plan, el mismo debe ser aprobado por el CGS.

Marco para la Planificación de la Continuidad de las Actividades del Organismo

Se mantendrá un solo marco para los planes de continuidad de las actividades del Organismo, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento.

Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo. Cuando se identifiquen nuevos requerimientos, se modificarán los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los recursos de emergencia existentes.

El administrador de cada plan de continuidad será el encargado de coordinar las tareas definidas en el mismo.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 105 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

Estas modificaciones deben ser propuestas por el RSI para su aprobación.


El marco para la planificación de la continuidad de las actividades del Organismo, tendrá en cuenta los siguientes puntos:

- a) Prever las condiciones de implementación de los planes que describan el proceso a seguir (cómo evaluar la situación, qué personas estarán involucradas, etc.) antes de poner en marcha los mismos.
- b) Definir los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones del Organismo y/o la vida humana. Esto debe incluir disposiciones con respecto a la gestión de las relaciones públicas y a vínculos eficaces a establecer con las autoridades públicas pertinentes, por ejemplo, la policía, bomberos y autoridades locales.
- c) Realizar los procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales del Organismo o de servicios de soporte a ubicaciones transitorias alternativas, y para el restablecimiento de los procesos en los plazos requeridos.
- d) Redactar los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales del Organismo.
- e) Definir un cronograma de mantenimiento que especifique cómo y cuándo será probado el plan, y el proceso para el mantenimiento del mismo.
- f) Efectuar actividades de concientización e instrucción al personal, diseñadas para propiciar la comprensión de los procesos de continuidad de las actividades y garantizar que los procesos sigan siendo eficaces.
- g) Documentar las responsabilidades y funciones de las personas, describiendo los responsables de la ejecución de cada uno de los componentes del plan y las vías de contacto posibles. Se deben mencionar alternativas cuando corresponda. Es de suma importancia definir a un responsable de declarar el estado de contingencia, lo cual dará inicio al plan.

Los administradores de los planes de contingencia son:

Plan de Contingencia | Administrador

El cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad, deben contarse entre las responsabilidades de los administradores de cada plan. Las disposiciones de emergencia para servicios técnicos alternativos, como instalaciones de comunicaciones o de procesamiento de información, normalmente se cuentan entre las responsabilidades de los proveedores de servicios.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 106 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

17.1.2. Implementación de la continuidad de la seguridad de la información

Control


El Organismo debe establecer, documentar, implementar y mantener los procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.

Los responsables de procesos y recursos de información, con la asistencia del RSI, elaborarán los planes de contingencia necesarios para garantizar la continuidad de las actividades del Organismo. Estos procesos deben ser propuestos por al CGS.

El proceso de planificación de la continuidad de las actividades considerará los siguientes puntos:

- a) Identificar y acordar respecto a todas las funciones y procedimientos de emergencia.
- b) Analizar los posibles escenarios de contingencia y definir las acciones correctivas a implementar en cada caso.
- c) Implementar procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos. Se debe dedicar especial atención a la evaluación de las dependencias de actividades externas y a los contratos vigentes.
- d) Documentar los procedimientos y procesos acordados.
- e) Instruir adecuadamente al personal, en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis.
- f) instruir al personal involucrado en los procedimientos de reanudación y recuperación en los siguientes temas:
 - 1) Objetivo del plan.
 - 2) Mecanismos de coordinación y comunicación entre equipos (personal involucrado).
 - 3) Procedimientos de divulgación.
 - 4) Requisitos de la seguridad.
 - 5) Procesos específicos para el personal involucrado.
 - 6) Responsabilidades individuales.
- g) Probar y actualizar los planes, guardando evidencia formal de las pruebas y sus resultados.

Asimismo, el proceso de planificación debe concentrarse en los objetivos de las actividades requeridas del Organismo, por ejemplo, restablecimiento de los servicios a los usuarios en un plazo aceptable. Deben considerarse los servicios y recursos que permitirán que esto ocurra, incluyendo, dotación de personal, recursos que no procesan información, así como acuerdos para reanudación de emergencia en sitios alternativos de procesamiento de la información.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 107 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

17.1.3. Verificación, revisión y valoración de la continuidad de la seguridad de la información

Control

El Organismo debe verificar a intervalos regulados los controles de continuidad de seguridad de la información establecidos e implementados para asegurar que sean válidos y eficaces durante situaciones adversas.

Los cambios organizacionales, técnicos, de procedimiento y de proceso, ya sea en un contexto operacional o de continuidad, pueden conducir a cambios en los requisitos de continuidad de seguridad de la información. En tales casos, la continuidad de los procesos, procedimientos y controles para la seguridad de la información deberán revisarse frente a estos requisitos cambiados.

El Organismo debe verificar su gestión de la continuidad de la seguridad de la información:


- a) ejercitando y probando la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información para asegurar que son coherentes con los objetivos de continuidad de seguridad de la información;
- b) ejercitando y probando el conocimiento y la rutina para operar los procesos, procedimientos y controles de continuidad de la seguridad de la información para asegurar que su desempeño es coherente con los objetivos de continuidad de seguridad de la información;
- c) revisando la validez y eficacia de las medidas de continuidad de la seguridad de la información cuando los sistemas de información, los procesos, procedimientos y controles de seguridad de la información o los procesos de continuidad de gestión de recuperación ante desastres y las soluciones para el cambio.

Debido a que los planes de continuidad de las actividades del Organismo pueden fallar, por suposiciones incorrectas, errores o cambios en el equipamiento, se establecen las siguientes pautas de acción:

- a) CGS junto al RSI establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.
- b) El cronograma indicará quienes son los responsables de llevar a cabo cada una de las pruebas y de elevar el resultado obtenido al citado Comité.

Se deben utilizar diversas técnicas para garantizar que los planes de contingencia funcionarán ante un hecho real, y éstas incluirán por lo menos:

- a) Efectuar pruebas de discusión de diversos escenarios (discutiendo medidas para la recuperación las actividades utilizando ejemplos de interrupciones).

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 108 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- b) Realizar simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis).
- c) Efectuar pruebas de recuperación técnica (garantizando que los sistemas de información puedan ser restablecidos con eficacia).
- d) Realizar ensayos completos probando que el Organismo, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones.

Para las operaciones críticas del Organismo se tomarán en cuenta, además, los siguientes mecanismos:

- a) Efectuar pruebas de recuperación en un sitio alternativo (ejecutando los procesos de las actividades del Organismo en paralelo, con operaciones de recuperación fuera del sitio principal).
- b) Realizar pruebas de instalaciones y servicios de proveedores (garantizando que los productos y servicios de proveedores externos cumplan con los compromisos contraídos).

Todas las pruebas efectuadas deben ser documentadas, resguardándose la evidencia formal de la ejecución y de los resultados obtenidos.

Los planes de continuidad de las actividades del Organismo serán revisados y actualizados periódicamente, para garantizar su eficacia permanente. Se incluirán procedimientos en el programa de administración de cambios del Organismo para garantizar que se aborden adecuadamente los tópicos de continuidad de las actividades.


La periodicidad de revisión de los planes de contingencia es la siguiente:

Plan de Contingencia | Revisar cada | Responsable de Revisión

Cada uno de los Responsables de Procesos es el responsable de las revisiones periódicas de cada uno de los planes de continuidad de su incumbencia, como así también de la identificación de cambios en las disposiciones relativas a las actividades del Organismo aún no reflejadas en dichos planes.

Debe prestarse atención, especialmente, a los cambios de:

- a) Personal.
- b) Direcciones o números telefónicos.
- c) Estrategia del Organismo.
- d) Ubicación, instalaciones y recursos.
- e) Legislación.
- f) Personal contratado, proveedores y clientes críticos.
- g) Procesos, o procesos nuevos / eliminados.
- h) Tecnologías.
- i) Requisitos operacionales.
- j) Requisitos de seguridad.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 109 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- k) Hardware, software y otros equipos (tipos, especificaciones, y cantidad).
- l) Requerimientos de los sitios alternativos.
- m) Registros de datos vitales.

Todas las modificaciones efectuadas serán propuestas por el RSI.

Por otra parte, el resultado de este proceso será dado a conocer a fin de que todo el Personal involucrado tenga conocimiento de los cambios incorporados.

17.2. Categoría: Redundancias

Objetivo de control

Asegurar la disponibilidad de las instalaciones de procesamiento de la información.

17.2.1. Disponibilidad de las instalaciones de procesamiento de la información

Control

Las instalaciones de procesamiento de la información se deben implementar con redundancia suficiente para cumplir con los requisitos de disponibilidad.

Para cumplir, el Organismo debe identificar los requisitos funcionales para considerar los componentes o arquitecturas redundantes. Hay que tener en cuenta durante el diseño, la actividad de la gestión de los riesgos de integridad y confidencialidad de la información que puedan acarrear las redundancias.

18. Cláusula: Cumplimiento


Responsabilidad

El RSI es responsable de definir normas y procedimientos para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual y a la conservación de registros. Realizar revisiones periódicas de los procesos de manejo de información del Organismo con el fin de verificar la correcta implementación de los controles de seguridad propuestos por la política de seguridad vigente.

Los RPI brindarán apoyo a la revisión periódica del cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables.

18.1. Categoría: Cumplimiento de los requisitos legales y contractuales

Objetivo de control

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 110 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

Evitar la violación de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y de cualquier requisito de seguridad.

18.1.1. Identificación de la legislación y de los requisitos contractuales aplicables.

Control

Todos los requisitos legales, estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque del Organismo para cumplir con estos requisitos, se deben identificar explícitamente, documentar y mantener actualizados para cada sistema de información, y para el Organismo.

El CGS deberá identificar todas las leyes aplicables al Organismo a fin de cumplir con los requisitos en función de su objeto.


18.1.2. Derechos de propiedad intelectual

Control

Se deben implementar los procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software propietarios.

Se debe considerar las siguientes recomendaciones para proteger cualquier material que pueda ser considerado propiedad intelectual:

- a) publicar una política o Normativa de cumplimiento de propiedad intelectual que defina el uso legal de los productos de software e información;
- b) adquirir software sólo de fuente conocidas y de buena reputación, para asegurar que los derechos de copia del software no han sido violados;
- c) mantener la concientización de las políticas de proteger los derechos de propiedad intelectual y publicando la intención de adoptar medidas disciplinarias para el personal que los viole;
- d) mantener un registro apropiado de activos, e identificar todos los activos con requisitos protegidos por el derecho de propiedad intelectual;
- e) mantener los documentos que acrediten la propiedad de licencias, discos originales, manuales, etc.;
- f) implantar controles para asegurar que no se sobrepasa el número máximo de usuarios permitidos de la licencia;
- g) llevar a cabo revisiones que solo son instalados productos de software autorizados y con licencia;

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 111 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

- h) establecer una política de mantenimiento de las condiciones adecuadas de licencia;
- i) establecer una política de eliminación de software o de su transferencia a terceros;
- j) cumplir con los términos y condiciones de uso del software y de la información obtenida de redes públicas;
- k) no duplicar, ni convertir a otro formato o extraer información de las grabaciones comerciales {película, audio) con excepción de lo permitido por los derechos de copia;
- l) no copiar total o parcialmente, libros, artículos, informes u otros documentos, con excepción de lo permitido por los derechos de copia.

Los derechos de propiedad intelectual incluyen software o documentos con derecho de copia, derechos de diseño, marcas registradas, patentes y código fuente licenciado.

Los productos de software propietario se suelen entregar con un contrato de licencia que especifica términos y condiciones del licenciamiento, por ejemplo, limitar el uso de los productos a máquinas específicas o limitar la generación de copias únicamente a finalidades de respaldo.

La importancia y la concienciación de los derechos de propiedad intelectual deberán comunicarse al personal para el software desarrollado por el Organismo.

Los requisitos legales, normativos y contractuales pueden plantear restricciones a la copia de material propietario. En particular, pueden requerir que sólo pueda utilizarse material desarrollado por el Organismo o bien proporcionado por el proveedor y bajo su licencia para el Organismo. La infracción de derechos de copia puede conducir a acciones legales que impliquen procedimientos judiciales.


18.1.3. Protección de los registros

Control

Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado o divulgación no autorizada, de acuerdo con los requisitos legales, reglamentarios, contractuales y de gestión.

Para la protección de los registros específicos del Organismo, debe considerarse la clasificación correspondiente basada en el esquema de la clasificación vigente.

Los registros se deben categorizar según el tipo, como, por ejemplo: registros contables, registros de base de datos, registros de transacciones, registros de auditorías y procedimientos operativos, cada uno de los cuales, con los detalles de retención y medios de almacenamiento, como, por ejemplo, papel, medios magnéticos u ópticos.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 112 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

Las claves criptográficas asociadas con archivos cifrados se mantendrán en forma segura y estarán disponibles para su uso por parte de personas autorizadas cuando resulte necesario.

Se debe considerar la posibilidad de degradación de los medios utilizados para el almacenamiento de los registros. Los procedimientos de almacenamiento y manipulación se implementarán de acuerdo con las recomendaciones del fabricante.

Si se seleccionan medios de almacenamiento electrónicos, se incluirán los procedimientos para garantizar la capacidad de acceso a los datos (tanto legibilidad de formato como medios) durante todo el período de retención, a fin de salvaguardar los mismos contra eventuales pérdidas ocasionadas por futuros cambios tecnológicos.

Deben elegirse los sistemas de almacenamiento tal que los datos requeridos puedan recuperarse de manera aceptable en tiempo y forma, dependiendo de los requisitos a satisfacer.

El sistema de almacenamiento y utilización debe asegurar la identificación de los registros y de su período de retención según lo definido por la legislación o las regulaciones nacionales o regionales, si es aplicable. Este debe permitir la destrucción apropiada de los registros tras dicho período cuando ya no los necesite el Organismo.

Para alcanzar los objetivos de salvaguardar los registros, deberán tomarse las siguientes medidas dentro de una organización:

- a) deberán publicarse directrices sobre la retención, almacenamiento, tratamiento y eliminación de los registros y la información;
- b) deberán establecerse un calendario de retenciones que identifique los registros y los períodos de tiempo que deberán retenerse;
- c) deberán mantenerse un inventario de las fuentes de información clave.


18.1.4. Privacidad y protección de la información personal

Control

Se debe asegurar la privacidad y la protección de la información personal, según lo requiera la legislación y regulación pertinente, cuando corresponda.

Se debe desarrollar e implementar una política o normativa de protección y de privacidad de los datos del Organismo; y ésta debe ser comunicada a todas las personas implicadas en el procesamiento de información personal.

Para el cumplimiento de esta política y de toda la legislación y regulaciones relevantes a la protección de la privacidad de las personas y datos personales, se requiere una apropiada estructura de gestión y control.

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 113 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

La responsabilidad de manejar información personal y de asegurar el conocimiento de los principios de privacidad, deberá establecerse de acuerdo con la legislación y regulaciones relevantes.

El Organismo redactará un “Compromiso de Confidencialidad”, el cual debe ser suscrito por todos los funcionarios públicos y personal contratado. La copia firmada del compromiso será retenida en forma segura por el Organismo.

Mediante este instrumento el empleado se comprometerá a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del Responsable del Activo de que se trate. A través del “Compromiso de Confidencialidad” se debe advertir al empleado que determinadas actividades pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

18.1.5. Regulación de controles criptográficos

Control

Los controles criptográficos se deben utilizar cumpliendo todos los acuerdos, leyes y regulaciones pertinentes.

Los siguientes puntos deben considerarse para el cumplimiento de los acuerdos, las leyes, y las regulaciones relevantes:

- a) restricciones en la importación o en la exportación de hardware y de software para realizar funciones criptográficas;
- b) restricciones en la importación o en la exportación de hardware y de software que se diseña para tener funciones criptográficas incluidas en él;
- c) restricciones en el uso de cifrado;
- d) métodos obligatorios o fijados a discreción de acceso por parte de las autoridades de los países a la información cifrada mediante hardware o software para proporcionar la confidencialidad del contenido.


18.2. Categoría: Revisión de la seguridad de la información

Objetivo de control

Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos del Organismo.

18.2.1. Revisión independiente de la seguridad de la información

Control

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 114 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

El enfoque del Organismo para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se debe revisar en forma independiente a intervalos planificados o cuando ocurran cambios significativos.

El CGS debe iniciar la revisión independiente. Tal revisión independiente, es necesaria para asegurar la conveniencia, adecuación y eficacia continuas del enfoque del Organismo para gestionar la seguridad de la información. La revisión debe incluir oportunidades de evaluación para la mejora y la necesidad de cambios en el enfoque de seguridad, incluyendo la política y los objetivos de control.

Dicha revisión debe realizarse por personas independientes del área bajo revisión. Las personas que lleven a cabo estas revisiones, deben tener las habilidades y experiencia apropiadas.

Los resultados de una revisión independiente deben registrarse y comunicarse a la gestión que inició la revisión. Estos registros deberán mantenerse.

Si la revisión independiente identifica que el enfoque del Organismo y la implementación para gestionar la seguridad de la información son inadecuados, el CGS deberá considerar las acciones correctivas.

18.2.2. Cumplimiento de las políticas y las normas de seguridad

Control


El nivel gerencial debe revisar periódicamente que el cumplimiento de los procesos y procedimientos de información en su área de responsabilidad, se alinee con las políticas, las normas y cualquier otro requisito de seguridad apropiados.

El CGS debe identificar cómo revisar si se cumplen los requisitos de seguridad de la información definidos en las políticas, normas y en otras regulaciones aplicables. Deben considerarse la medición automática y las herramientas de informes para una revisión periódica eficiente.

Si algún incumplimiento se encuentra como resultado de la revisión, el CGS deberá:

- a) identificar las causas del incumplimiento;
- b) evaluar la necesidad de tomar medidas para lograr el cumplimiento;
- c) implementar las acciones correctivas apropiadas;
- d) revisar la acción correctiva tomada para comprobar su eficacia e identificar las deficiencias y debilidades.

Los resultados de las revisiones y de las acciones correctivas realizadas, deben registrarse y estos registros deben mantenerse. El CGS debe reportar los

Código: L_SGDS_001_PSI_INTI Ver/Rev.: 1.0 Conf.: Reserv. Uso Interno Página: 115 de 115	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	 INTI 65 Años 1957-2022 Instituto Nacional de Tecnología Industrial
SUBGERENCIA OPERATIVA DE INFORMÁTICA		

resultados a las personas que realizan las revisiones independientes, cuando la revisión independiente se realice en el área de su responsabilidad.

18.2.3. Revisión del cumplimiento técnico

Control

Los sistemas de información se deben revisar periódicamente para verificar que cumplan con las políticas y las normas de seguridad de la información del Organismo.

El cumplimiento técnico debe realizarse preferente con la ayuda de herramientas automatizadas que generen un informe técnico para su posterior interpretación por un especialista técnico.

Si se utilizan pruebas de intrusión o evaluaciones de vulnerabilidad, deberá tenerse cuidado pues estas actividades podrían comprometer la seguridad del sistema. Tales pruebas deberán planificarse, documentarse y repetirse.

Cualquier revisión del cumplimiento técnico deberán realizarse solamente por las personas competentes, autorizadas, o bajo supervisión de tales personas.

La revisión del cumplimiento técnico comprende el examen de los sistemas operacionales a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados. Este tipo de revisión de la conformidad requiere asistencia técnica especializada.

La revisión del cumplimiento también comprende, por ejemplo, pruebas de intrusión y evaluación de vulnerabilidades, las cuales podrían ser realizadas por expertos independientes contratados específicamente con este propósito. Esto puede resultar útil para la detección de vulnerabilidades en el sistema y para verificar la eficacia de los controles con relación a la prevención de accesos no autorizados posibilitados por las mismas.

Las pruebas de intrusión y la evaluación de vulnerabilidades proporcionan una muestra de un sistema en un estado y momento específico. La muestra se limita a esas porciones del sistema probado realmente durante el o los intentos de penetración. Las pruebas de intrusión y la evaluación de vulnerabilidades no son un sustituto para la evaluación de riesgo.



República Argentina - Poder Ejecutivo Nacional
1983/2023 - 40 AÑOS DE DEMOCRACIA

Hoja Adicional de Firmas
Informe gráfico

Número:

Referencia: Política de seguridad de la información

El documento fue importado por el sistema GEDO con un total de 115 pagina/s.