POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA SUBSECRETARÍA DE ESTADO DE ADMINISTRACIÓN FINANCIERA

Versión 2

Tabla de Contenido

1. Política de Seguridad de la Información 7

1.1. Política de Seguridad de la información 8

1.1.1. Documento de la política de seguridad de la información 8

1.1.1. Revisión de la política de seguridad de la información 9

2. Organización de la Seguridad 10

2.1. Organización interna 11

2.1.1. Compromiso de la dirección con la seguridad de la información 11

2.1.2. Coordinación de la seguridad de la información 11

2.1.3. Autorización para Instalaciones de Procesamiento de Información 12

2.1.4. Acuerdos de confidencialidad 12

2.1.5. Contacto con otros Organismos 12

2.1.6. Contacto con grupos de interés especial 13

2.1.7. Revisión independiente de la seguridad de la información 13

2.2. Grupos o personas externas 13

2.2.1. Identificación de los riesgos relacionados con grupos externos 13

2.2.2. Puntos a considerar en Contratos o Acuerdos con terceros 14

2.2.3. Puntos a ser considerados en acuerdos con terceros 15

3. Gestión de Activos 17

3.1. Responsabilidad sobre los activos 18

3.1.1. Inventario de activos 18

3.1.2. Propiedad de los activos 19

3.1.3. Uso aceptable de los activos 19

3.2. Clasificación de la información 19

3.2.1. Directrices de clasificación 20

3.2.2. Etiquetado y manipulado de la información 21

4. Recursos Humanos 22

4.1. Antes del empleo 23

4.1.1. Funciones y responsabilidades 23

4.1.2. Términos y condiciones de contratación 23

4.2. Durante el empleo 23

4.2.1. Responsabilidad de la SSEAF 23

4.3. Cese del empleo o cambio de puesto de trabajo 24

4.3.1. Responsabilidad del cese o cambio 24

4.3.2. Devolución de Activos 24

4.3.3. Retiro de los Derechos de Acceso 24

5. Seguridad Física y Ambiental 25

5.1. Áreas Seguras 26

5.1.1. Perímetro de seguridad física 26

5.1.2. Controles físicos de entrada 27

5.1.3. Seguridad de oficinas, despachos, instalaciones 28
5.1.4. Protección contra amenazas externas y de origen ambiental 29
5.1.5. Trabajo en áreas seguras 29
5.1.6. Áreas de acceso público, de carga y descarga 30

5.2. Seguridad de los equipos 30
5.2.1. Ubicación y Protección del Equipamiento 30
5.2.2. Instalaciones de suministro 31
5.2.3. Seguridad del Cableado 32
5.2.4. Mantenimiento de Equipos 32
5.2.5. Seguridad de los Equipos Fuera de las Instalaciones. 32
5.2.6. Reutilización o retiro seguro de equipos 33
5.2.7. Retirada de materiales propiedad de la empresa 33
5.2.8. Políticas de Escritorios y Pantallas Limpias. 33

6. Gestión de Comunicaciones y Operaciones 35

6.1. Procedimientos y Responsabilidades Operativas 37
6.1.1. Documentación de los Procedimientos Operativos 37
6.1.2. Cambios en las Operaciones 38
6.1.3. Separación de Funciones 38
6.1.4. Separación entre Instalaciones de Desarrollo e Instalaciones Operativas 39

6.2. Gestión de Provisión de Servicios 39
6.2.1. Provisión de servicio 39
6.2.2. Seguimiento y revisión de los servicios de las terceras partes 40
6.2.3. Gestión del cambio de los servicios de terceras partes 40

6.3. Planificación y Aprobación de Sistemas 41
6.3.1. Planificación de la Capacidad 41
6.3.2. Aprobación del Sistema 41

6.4. Protección Contra Código Malicioso 42
6.4.1. Código Malicioso 42

6.5. Respaldo o Back-up 43
6.5.1. Resguardo de la Información 43
6.5.2. Registro de Actividades del Personal Operativo 44
6.5.3. Registro de Fallas 44

6.6. Gestión de la Red 44
6.6.1. Redes 45

6.7. Administración y Seguridad de los medios de almacenamiento 45
6.7.1. Administración de Medios Informáticos Removibles 45
6.7.2. Eliminación de Medios de Información 46
6.7.3. Procedimientos de Manejo de la Información 46
6.7.4. Seguridad de la Documentación del Sistema 47

6.8. Intercambios de Información y Software 47
6.8.1. Procedimientos y controles de intercambio de la información 47
6.8.2. Acuerdos de Intercambio de Información y Software 48
6.8.3. Seguridad de los Medios en Tránsito 48
6.8.4. Seguridad de la Mensajería 49

6.9. Seguridad del Correo Electrónico 49
6.9.1. Riesgos de Seguridad 49
6.9.2. Política de Correo Electrónico 50
6.9.3. Seguridad de los Sistemas Electrónicos de Oficina 51
6.9.4. Sistemas de Acceso Público 51
6.9.5. Otras Formas de Intercambio de Información 52

6.10. Seguimiento y control 53
6.10.1. Registro de auditoría 53
6.10.2. Protección de los registros 54
6.10.3. Registro de actividad de administrador y operador 54
6.10.4. Sincronización de Relojes 54

7. Gestión de Accesos 55

7.1. Requerimientos para el Control de Acceso 57
7.1.1. Política de Control de Accesos 57
7.1.2. Reglas de Control de Acceso 58

7.2. Administración de Accesos de Usuarios 58
7.2.1. Registración de Usuarios 58
7.2.2. Gestión de Privilegios 59
7.2.3. Gestión de Contraseñas de Usuario 60
7.2.4. Administración de Contraseñas Críticas 61
7.2.5. Revisión de Derechos de Acceso de Usuarios 61

7.3. Responsabilidades del Usuario 61
7.3.1. Uso de Contraseñas 62
7.3.2. Equipos Desatendidos en Áreas de Usuarios 63

7.4. Control de Acceso a la Red 63
7.4.1. Política de Utilización de los Servicios de Red 63
7.4.2. Camino Forzado 64
7.4.3. Autenticación de Usuarios para Conexiones Externas 64
7.4.4. Autenticación de Nodos 65
7.4.5. Protección de los Puertos (Ports) de Diagnóstico Remoto 65
7.4.6. Subdivisión de Redes 65
7.4.7. Acceso a Internet 66
7.4.8. Conexión a la Red 66
7.4.9. Ruteo de Red 66
7.4.10. Seguridad de los Servicios de Red 67

7.5. Control de Acceso al Sistema Operativo 67
7.5.1. Identificación Automática de Terminales 67
7.5.2. Procedimientos de Conexión de Terminales 68
7.5.3. Identificación y Autenticación de los Usuarios 68
7.5.4. Sistema de Administración de Contraseñas 69
7.5.5. Uso de Utilitarios de Sistema 69
7.5.6. Desconexión de Terminales por Tiempo Muerto 70
7.5.7. Limitación del Horario de Conexión 70

7.6. Control de Acceso a las Aplicaciones 71
7.6.1. Restricción del Acceso a la Información 71

7.6.2. Aislamiento de los Sistemas Sensibles 72

7.7. Monitoreo del Acceso y Uso de los Sistemas 72

7.7.1. Registro de Eventos 72
7.7.2. Procedimientos y Áreas de Riesgo 73
7.7.3. Registro y Revisión de Eventos 74

7.8. Dispositivos Móviles y Trabajo Remoto 75

7.8.1. Computación Móvil 75
7.8.2. Trabajo Remoto 76

8. Desarrollo y Mantenimiento de Sistemas 79

8.1. Requerimientos de Seguridad de los Sistemas 80

8.1.1. Análisis y Especificaciones de los Requerimientos de Seguridad 80

8.2. Seguridad en los Sistemas de Aplicación 81

8.2.1. Validación de Datos de Entrada 81
8.2.2. Controles de Procesamiento Interno 82
8.2.3. Autenticación de Mensajes 82
8.2.4. Validación de Datos de Salidas 82

8.3. Controles Criptográficos 82

8.3.1. Política de Utilización de Controles Criptográficos. 83
8.3.2. Cifrado 83
8.3.3. Firma Digital 83
8.3.4. Servicios de No Repudio 84
8.3.5. Protección de Claves Criptográficas 84
8.3.6. Protección de Claves Criptográficas: Normas y Procedimientos 84

8.4. Seguridad de los Archivos del Sistema 85

8.4.1. Software Operativo 85
8.4.2. Protección de los Datos de Prueba del Sistema 86
8.4.3. Control de Cambios a Datos Operativos 86
8.4.4. Control de Acceso a las Bibliotecas de Programas Fuentes 87

8.5. Seguridad de los Procesos de Desarrollo y Soporte 88

8.5.1. Procedimiento de Control de Cambios 88
8.5.2. Revisión Técnica de los Cambios en el Sistema Operativo 89
8.5.3. Restricción del Cambio de Paquetes de Software 89
8.5.4. Canales Ocultos y Código Malicioso 89
8.5.5. Desarrollo Externo de Software 90

8.6. Gestión de vulnerabilidades técnicas 90

8.6.1. Vulnerabilidades técnicas 90

9. Gestión de Incidentes de Seguridad 92

9.1. Informe de los eventos y debilidades de la seguridad de la información 92

9.1.1. Reporte de los eventos de la seguridad de información 92
9.1.2. Reporte de las debilidades de la seguridad 93
9.1.3. Comunicación de Anomalías del Software 93

9.2. Gestión de los Incidentes y mejoras de la seguridad de la información 93

9.2.1. Responsabilidades y procedimientos 94
9.2.2. Aprendiendo a partir de los incidentes de la seguridad de la información 95
9.2.3. Procesos Disciplinarios 95

10. Gestión de la Continuidad 96

10.1. Categoría: Gestión de continuidad del Organismo 97
10.1.1. Proceso de Administración de la Continuidad de la SSEAF 97
10.1.2. Continuidad de las Actividades y Análisis de los Impactos 98
10.1.3. Elaboración e Implementación de los Planes de Continuidad de la SSEAF 98
10.1.4. Marco para la Planificación de la Continuidad de las Actividades de la SSEAF 99
10.1.5. Ensayo, Mantenimiento y Reevaluación de los Planes de Continuidad de la SSEAF... 100

11. Cumplimiento 103

11.1. Cumplimiento de Requisitos Legales 104
11.1.1. Identificación de la Legislación Aplicable 104
11.1.2. Derechos de Propiedad Intelectual 104
11.1.3. Protección de los Registros de la SSEAF 105
11.1.4. Protección de Datos y Privacidad de la Información Personal 106
11.1.5. Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información . 106
11.1.6. Recolección de Evidencia 107

11.2. Revisiones de la Política de Seguridad y la Compatibilidad Técnica 107
11.2.1. Cumplimiento de la Política de Seguridad 107
11.2.2. Verificación de la Compatibilidad Técnica 108

11.3. Sanciones Previstas por Incumplimiento 108

1. Política de Seguridad de la Información

Generalidades

La información es un recurso que, como el resto de los activos, tiene valor para la SSEAF y por consiguiente debe ser debidamente protegida.

Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la SSEAF.

Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional.

Para esto, se debe asegurar un compromiso manifiesto de las máximas Autoridades de la SSEAF y de sus Direcciones dependientes para la difusión, consolidación y cumplimiento de la presente Política.

Objetivo

Proteger los recursos de información de la SSEAF y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.

Mantener la Política de Seguridad de la SSEAF actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

Alcance

Esta Política se aplica en todo el ámbito de la SSEAF, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Responsabilidad

Todos los Directores, Coordinadores, Jefes de Departamento, o equivalentes son responsables de la implementación de esta Política de Seguridad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la SSEAF, cualquiera sea su situación de dependencia, el área al cual se encuentre afectada y cualquiera sea el nivel de las tareas que desempeñe.

Las máximas autoridades de la SSEAF aprueban esta Política y son responsables de la autorización de sus modificaciones.

Los **Propietarios de la Información**[1] son responsables de clasificarla de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia. Está función será ejercida por las **Direcciones de la SSEAF**.

La **Dirección General de Informática y Comunicaciones (DGIC)** cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la SSEAF. Por otra parte tendrá la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

El **Departamento de Seguridad de la Información de la DGIC** cumplirá funciones relativas a la seguridad de los sistemas de información de la SSEAF, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política.

Los **usuarios de la información y de los sistemas** utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.

Política

1.1. Política de Seguridad de la información

Objetivo

Proporcionar a la SSEAF la dirección y soporte para la seguridad de la información en concordancia con los requerimientos, las leyes y regulaciones relevantes. La SSEAF debe establecer claramente la dirección de la política en línea con los objetivos.

1.1.1. Documento de la política de seguridad de la información

El documento de la política debe ser aprobado por la SSEAF, publicado y comunicado a todos los empleados y las partes externas relevantes.

Esta Política se conforma de una serie de pautas sobre aspectos específicos de la Seguridad de la Información, que incluyen los siguientes tópicos:

- Organización de la Seguridad
  Orientado a administrar la seguridad de la información dentro de la SSEAF y establecer un marco gerencial para controlar su implementación.
- Gestión de Activos
  Destinado a mantener una adecuada protección de los activos de la SSEAF.
- Recursos Humanos
  Orientado a reducir los riesgos de error humano, comisión de ilícitos contra la SSEAF o uso inadecuado de instalaciones.

[1] El concepto "Propietario de la Información" debe ser entendido desde su acepción técnica, no jurídica.

- Seguridad Física y Ambiental
  Destinado a impedir accesos no autorizados, daños e interferencia a las sedes e información de la SSEAF.
- Gestión de Comunicaciones y Operaciones
  Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.
- Gestión de Accesos
  Orientado a controlar el acceso lógico a la información.
- Desarrollo y Mantenimiento de Sistemas
  Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento.
- Gestión de Incidentes de Seguridad
  Orientado a administrar todos los eventos que atenten contra la confidencialidad, integridad y disponibilidad de la información y los activos tecnológicos.
- Gestión de la Continuidad
  Orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.
- Cumplimiento
  Destinado a impedir infracciones y violaciones de las normativas legales vigentes. Revisión de la política de seguridad de la información

La máxima autoridad de la SSEAF aprobará formalmente la Política y la comunicará a todos los empleados y terceras partes relevantes.

1.1.1. Revisión de la política de seguridad de la información

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

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

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

2. Organización de la Seguridad

Generalidades

La presente Política de Seguridad establece la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la SSEAF.

Por ello, se definirá formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades.

Asimismo, se contemplará 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 de la SSEAF 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 considerará 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 establecerán las medidas adecuadas para la protección de la información.

Objetivo

Administrar la seguridad de la información dentro de la SSEAF y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

Fomentar la consulta y cooperación con Organismos especializados para la obtención de asesoría en materia de seguridad de la información.

Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información de la SSEAF.

Alcance

Esta Política se aplica a todos los recursos de la SSEAF y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

Responsabilidad

El Director de la DGIC en coordinación con las áreas de Seguridad Informática serán responsables de impulsar la implementación de la presente Política.

Se debe garantizar la autonomía del Área de Seguridad en la aplicación de esta Política.

El Departamento de Seguridad de la Información asistirá al personal de la SSEAF en materia de seguridad de la información y coordinará la interacción con Organismos especializados. Asimismo, junto con los propietarios de la información, analizará el riesgo de los accesos de terceros a la información de la SSEAF y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma.

Las Direcciones de la SSEAF cumplirán la función de autorizar la incorporación de nuevos recursos de procesamiento de información a las áreas de su incumbencia.

La DGIC controlará que 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, se incluya la obligatoriedad del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas relacionadas.

El Responsable del Área Legal de la SSEAF participará en dicha tarea.

Asimismo, notificará a los proveedores sobre las modificaciones que se efectúen a la Política de Seguridad de la Información de la SSEAF.

Política

2.1. Organización interna

Objetivo

Manejar la seguridad de la información dentro del organismo.

Se debe establecer un marco referencial gerencial o política, para iniciar y controlar la implementación de la seguridad de la información dentro del organismo.

La SSEAF debe aprobar la política de seguridad de la información, asignar los roles de seguridad, coordinar y revisar la implementación de la seguridad en todo el organismo.

2.1.1. Compromiso de la dirección con la seguridad de la información

La SSEAF debe apoyar la seguridad de la información a través de una dirección clara, mostrando compromiso, asignando roles y reconociendo responsabilidades explícitas.

Debe formular, revisar y aprobar la política de seguridad de la información, como asimismo revisar los beneficios de la implementación de la misma.

La seguridad de la información es una responsabilidad de la SSEAF compartida por todas las Autoridades, Directores o Generales, Coordinadores, Jefes, o equivalentes.

2.1.2. Coordinación de la seguridad de la información

La coordinación de la seguridad de la información debiera involucrar la cooperación y colaboración de la máxima autoridad de la SSEAF, incluyendo: los Directores Generales, Coordinadores, Jefes, o equivalentes, usuarios, administradores, diseñadores de aplicación, auditores y personal de seguridad, y áreas especializadas como seguros, asesorías legales, recursos humanos, TI o gestión del riesgo. Esta actividad debiera:

a) asegurar que las actividades de seguridad sean ejecutadas en conformidad con la política de seguridad de la información;

b) identificar cómo manejar las no-conformidades;

c) aprobar las metodologías y procesos para la seguridad de la información; por ejemplo, la evaluación del riesgo, la clasificación de la información;

d) identificar cambios significativos en las amenazas y la exposición de la información y los medios de procesamiento de la información ante amenazas;

e) evaluar la idoneidad y coordinar la implementación de los controles de la seguridad de información;

f) promover de manera efectiva la educación, capacitación y conocimiento de la seguridad de la información a través de toda la organización;

g) evaluar la información recibida del monitoreo y revisar los incidentes de seguridad de la información, y recomendar las acciones apropiadas en respuesta a los incidentes de seguridad de información identificados.

2.1.3. Autorización para Instalaciones de Procesamiento de Información

Los nuevos recursos de procesamiento de información serán autorizados por los Responsables de las Direcciones involucradas, considerando su propósito y uso, conjuntamente con la Dirección de la DGIC y el Departamento de Seguridad de la Información, a fin de garantizar que se cumplan todas las Políticas y requerimientos de seguridad pertinentes.

Las siguientes guías deben ser consideradas para el proceso de autorización:

a) Cumplir con los niveles de aprobación vigentes en la SSEAF, asegurando el cumplimiento de las políticas y requerimientos.

b) Cuando corresponda, se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas de la SSEAF.

c) El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso será evaluado por el Departamento de Seguridad de la Información y autorizado, en cada caso, por el Dpto. de Soporte Técnico y por el Director (o equivalente) responsable del área al que se destinen los recursos.

2.1.4. Acuerdos de confidencialidad

Se definirán, implementarán y revisarán regularmente los acuerdos de confidencialidad o de no divulgación para la protección de la información de la SSEAF. Dichos acuerdos deben responder a los requerimientos de confidencialidad o no divulgación de la SSEAF, los cuales serán revisados periódicamente. Asimismo, deben cumplir con toda legislación o normativa que alcance a la SSEAF en materia de confidencialidad de la información.

Dichos acuerdos deben celebrarse tanto con el personal del organismo como con aquellos terceros que se relacionen de alguna manera con su información.

2.1.5. Contacto con otros Organismos

A efectos de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad, se mantendrán contactos con los Organismos nacionales o internacionales especializados en temas relativos a la seguridad informática.

En los intercambios de información de seguridad, no se divulgará información confidencial perteneciente a la SSEAF a personas no autorizadas.

El intercambio de información confidencial para fines de asesoramiento o de transmisión de experiencias, sólo se permite cuando se haya firmado un Compromiso de Confidencialidad previo con aquellas Organizaciones especializadas en temas relativos a la seguridad informática cuyo personal está obligado a mantener la confidencialidad de los temas que trata.

2.1.6. Contacto con grupos de interés especial

El Departamento de Seguridad de la Información será el encargado de coordinar los conocimientos y las experiencias disponibles en la SSEAF a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Este podrá obtener asesoramiento de otros Organismos. Con el objeto de optimizar su gestión, se habilitará al Departamento de Seguridad de la Información el contacto con todas las Dependencias de la SSEAF.

Se 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.

2.1.7. Revisión independiente de la seguridad de la información

La Auditoría Interna o en su defecto quien sea formalmente designado realizará revisiones independientes sobre la vigencia, implementación y gestión de la Política de Seguridad de la Información, a efectos de garantizar que las prácticas de la SSEAF reflejan adecuadamente sus disposiciones.

Estas revisiones deben incluir las oportunidades de evaluación de mejoras y las necesidades de cambios de enfoque en la seguridad, incluyendo políticas y objetivos de control.

Se deben registrar y reportar todas estas actividades.

2.2. Grupos o personas externas

Objetivo

Mantener la seguridad de la información y los medios de procesamiento de información de la SSEAF que son ingresados, procesados, comunicados , o manejados por grupos externos.

La seguridad de la información y los medios de procesamiento de la información de la SSEAF no deben ser reducidos por la introducción de productos y servicios de grupos externos.

2.2.1. Identificación de los riesgos relacionados con grupos externos

Cuando exista la necesidad de otorgar acceso a terceras partes a información de la SSEAF, el Departamento de Seguridad de la Información y el Propietario de la Información de que se trate, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

a) Los medios de procesamiento de información a los cuales necesita tener acceso el grupo externo.

b) El tipo de acceso requerido (físico/lógico y a qué recurso).

c) Los motivos para los cuales se solicita el acceso.

d) El valor de la información.

e) Los controles empleados por la tercera parte.

f) Diferentes medios y controles empleados por el grupo externo cuando almacena, procesa, comunica, comparte e intercambia información.

g) La incidencia de este acceso en la seguridad de la información de la SSEAF.

En todos los contratos o acuerdos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro de la SSEAF, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

Se cita a modo de ejemplo:

a) Personal de mantenimiento y soporte de hardware y software.

b) Limpieza, guardia de seguridad y otros servicios de soporte tercerizados.

c) Pasantías y otras designaciones de corto plazo.

d) Consultores.

e) Auditores

En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso.

2.2.2. Puntos a considerar en Contratos o Acuerdos con terceros

Se revisarán los contratos o acuerdos existentes o que se efectúen con terceros, teniendo en cuenta la necesidad de aplicar los siguientes controles:

a) Cumplimiento de la Política de seguridad de la información de la SSEAF.

b) Protección de los activos de la SSEAF, incluyendo:

- Procedimientos para proteger los bienes de la SSEAF, abarcando los activos físicos, la información y el software.
- Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
- Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.

- Restricciones a la copia y divulgación de información.

c) Descripción de los servicios disponibles.

d) Nivel de servicio esperado y niveles de servicio aceptables.

e) Permiso para la transferencia de personal cuando sea necesario.

f) Obligaciones de las partes emanadas del acuerdo y responsabilidades legales.

g) Existencia de Derechos de Propiedad Intelectual.

h) Definiciones relacionadas con la protección de datos.

i) Acuerdos de control de accesos que contemplen:

- Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
- Proceso de autorización de accesos y privilegios de usuarios.
- Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.

j) Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.

k) Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.

l) Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.

m) Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.

n) Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.

o) Proceso claro y detallado de administración de cambios.

p) Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.

q) Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.

r) Controles que garanticen la protección contra software malicioso.

s) Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.

t) Relación entre proveedores y subcontratistas.

2.2.3. Puntos a ser considerados en acuerdos con terceros

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 de la SSEAF, contemplarán además de los puntos especificados en el punto anterior, los siguientes aspectos:

a) Forma en que se cumplirán los requisitos legales aplicables.

b) Medios para garantizar que todas las partes involucradas en la tercerización, incluyendo los subcontratistas, están al corriente de sus responsabilidades en materia de seguridad.

c) Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos de la SSEAF.

d) Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible de la SSEAF.

e) Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.

f) Niveles de seguridad física que se asignarán al equipamiento tercerizado.

g) Derecho a la auditoría por parte de la SSEAF sobre los aspectos tercerizados en forma directa o a través de la contratación de servicios ad hoc.

Se debe prever la factibilidad de ampliar los requerimientos y procedimientos de seguridad con el acuerdo de las partes.

3. Gestión de Activos

Generalidades

La SSEAF debe tener un acabado conocimiento sobre los activos que posee como parte importante de la administración de riesgos. Algunos ejemplos de activos son:

a. Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc.

b. Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, etc.

c. Activos físicos: equipamiento informático (servidores, computadoras personales, computadoras portátiles, dispositivos de almacenamiento, etc.), equipos de comunicaciones (routers, switches, centrales telefónicas, etc.), medios magnéticos (cintas, discos, dispositivos móviles de almacenamiento de datos, pen drives, discos externos, etc.), otros equipos técnicos (generadores, UPS, unidades de aire acondicionado, sistemas de control de acceso, etc.), mobiliario, oficinas, etc.

d. Servicios: servicios informáticos y de comunicaciones, utilitarios generales (energía eléctrica, internet, etc.).

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable y que ésta puede cambiar de acuerdo con una Política predeterminada. Se debe considerar la cantidad de categorías a definir para la clasificación evitando esquemas demasiado complejos.

La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos. Puede ser almacenada (en dichos sistemas o en medios portátiles), transmitida (a través de redes o entre sistemas) e impresa o escrita en papel. Cada una de estas formas debe contemplar todas las medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información.

Por último, la información puede pasar a ser obsoleta y por lo tanto, ser necesario eliminarla. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

Objetivo

Garantizar que los activos de información reciban un apropiado nivel de protección.

Clasificar la información para señalar su sensibilidad y criticidad.

Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

Alcance

Esta Política se aplica a toda la información administrada en la SSEAF, cualquiera sea el soporte en que se encuentre.

Responsabilidad

Los Propietarios de los Activos son los encargados de clasificarlos de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, de definir quiénes pueden tener permisos de acceso a los activos y son responsables de mantener los controles adecuados para garantizar su seguridad.

El Departamento de Seguridad de la Información es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea realizado de acuerdo a lo establecido en la presente Política.

Política

3.1. Responsabilidad sobre los activos

Objetivo

Todos los activos deben ser inventariados y contar con un propietario nombrado.

Los propietarios deben identificar todos los activos y se deberá asignar la responsabilidad por el mantenimiento de los controles apropiados. La implementación de controles específicos puede ser delegada por el propietario conforme sea apropiado, pero el propietario sigue siendo responsable por la protección apropiada de los activos.

3.1.1. Inventario de activos

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información.

Se identificarán los activos de información del Organismo, incluyendo:

a. información: bases de datos, archivos de datos, documentación, contratos, acuerdos;

b. activos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo, y utilitarios;

c. activos físicos: equipamiento de computación, equipamiento de comunicaciones, medios removibles y otros equipamientos;

d. instalaciones: edificios, ubicaciones físicas, tendido eléctrico, red de agua, etc.;

e. servicios: servicios de cómputo y de comunicaciones, servicios generales, por ejemplo: energía, internet, telefonía;

f. personas, y sus calificaciones, habilidades y experiencia;

El inventario será actualizado ante cualquier modificación de la información registrada y revisado anualmente.

3.1.2. Propiedad de los activos

Toda la información y los activos junto a sus medios de procesamiento de información deben ser propiedad de un responsable designado por la SSEAF.

Se designarán los Propietarios de los activos identificados, quienes deben cumplir sus funciones de propietario, esto es:

a. informar sobre cualquier cambio que afecte el inventario de activos.
b. clasificar los activos en función a su valor.
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.

Cabe aclarar que, si bien los propietarios 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 propietarios de los activos será documentada por los mismos y proporcionada al Responsable de Seguridad de la Información.

3.1.3. Uso aceptable de los activos

Se identificarán, documentarán e implementarán reglas para el uso aceptable de la información y los activos asociados con las instalaciones de procesamiento de la información.

Todos los empleados, contratistas y usuarios de terceras partes deben seguir las reglas para el uso aceptable de la información y los activos asociados con las instalaciones de procesamiento de la misma, incluyendo:

a. correo electrónico,
b. sistemas de gestión,
c. estaciones de trabajo,
d. dispositivos móviles,
e. etc.

3.2. Clasificación de la información

Objetivo

Asegurar que la información reciba un nivel de protección apropiado.

La información debe ser clasificada para indicar la necesidad, prioridades y grado de protección esperado cuando se maneja la información.

La información tiene diversos grados de confidencialidad e importancia. Algunos ítems pueden requerir un nivel de protección adicional o manejo especial. Se debe utilizar un esquema de clasificación de información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de uso especiales.

3.2.1. Directrices de clasificación

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

A continuación se establece el criterio de clasificación de la información en función a cada una de las mencionadas características:

a. Confidencialidad:

1- PUBLICO: Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de la SSEAF o no.

2- USO INTERNO: Información que puede ser conocida y utilizada por todos los empleados de la SSEAF y algunas entidades externas debidamente autorizadas y cuya divulgación o uso no autorizados podría ocasionar riesgos o impactos leves a la SSEAF, o a terceros.

3- RESERVADA: Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo y cuya divulgación o uso no autorizados podría ocasionar impacto significativo a la SSEAF o a terceros.

b. Integridad:

1- Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operación de la SSEAF.

2- Información cuya modificación no autorizada puede repararse aunque podría ocasionar impacto leve a la SSEAF, o a terceros.

3- Información cuya modificación no autorizada es de difícil reparación y podría ocasionar impacto significativo a la SSEAF, o a terceros.

c. Disponibilidad:

1- Información cuya inaccesibilidad no afecta la operación de la SSEAF.

2- Información cuya inaccesibilidad permanente durante más de dos días podría ocasionar impacto significativo a la SSEAF, o a terceros.

3- Información cuya inaccesibilidad permanente durante más de dos horas podría ocasionar impacto significativo a la SSEAF, o a terceros.

Al referirse a pérdidas, se contemplan aquellas cuantificables (materiales) y no cuantificables (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, etc.).

Se asignará a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en una de las siguientes categorías:

- **CRITICIDAD BAJA**: ninguno de los valores asignados superan el 1.
- **CRITICIDAD MEDIA**: alguno de los valores asignados es 2
- **CRITICIDAD ALTA**: alguno de los valores asignados es 3

Sólo el Propietario de la Información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:

- Asignarle una fecha de vigencia.
- Comunicárselo al depositario del recurso.
- Realizar los cambios necesarios para que los Usuarios conozcan la nueva clasificación.

Luego de clasificada la información, el propietario de la misma identificará los recursos asociados (sistemas, equipamiento, servicios, etc.) y los perfiles funcionales que deberán tener acceso a la misma.

3.2.2. Etiquetado y manipulado de la información

Se definirán procedimientos para el rotulado y manejo de información, de acuerdo al esquema de clasificación definido. Los mismos contemplarán los recursos de información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información:

- Copia;
- Almacenamiento;
- Transmisión por correo, fax, correo electrónico;
- Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, etc.);
- Transmisión a través de mecanismos de intercambio de archivos (FTP, almacenamiento masivo remoto, etc.).

Para cada uno de los niveles de clasificación, se deben definir los procedimientos de manejo seguros, incluyendo las actividades de procesamiento, almacenaje, transmisión, desclasificación y destrucción.

4. Recursos Humanos

Generalidades

La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación laboral, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

Objetivo

Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la SSEAF en el transcurso de sus tareas normales.

Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.

Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

Alcance

Esta Política se aplica a todo el personal de la SSEAF, cualquiera sea su situación laboral, y al personal externo que efectúe tareas dentro del ámbito de la SSEAF.

Responsabilidad

La SSEAF incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los funcionarios, informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto de la presente Política.

La DGIC participará en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en la SSEAF, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de la presente Política y en el tratamiento de incidentes de seguridad que requieran de su intervención.

Política

4.1. Antes del empleo

Objetivo

Asegurar que los funcionarios, contratados y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de los medios.

Las responsabilidades de seguridad deben ser tratadas antes del empleo en las definiciones de trabajo adecuadas y en los términos y condiciones del empleo

4.1.1. Funciones y responsabilidades

Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo.

Estas incluirán las responsabilidades generales relacionadas con la implementación y el mantenimiento de la Política de Seguridad, y las responsabilidades específicas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.

Se definirán y comunicarán claramente los roles y responsabilidades de seguridad a los candidatos para el puesto de trabajo durante el proceso de preselección.

4.1.2. Términos y condiciones de contratación

Como parte de sus términos y condiciones iniciales de empleo, los funcionarios, cualquiera sea su situación laboral, 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 el Área de Recursos Humanos u otra competente.

Asimismo, mediante el Compromiso de Confidencialidad el funcionario 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 funcionario.

4.2. Durante el empleo

Objetivo

Asegurar que los usuarios, funcionarios, contratados y terceras personas estén al tanto de la seguridad de la información, sus responsabilidades y obligaciones, y estén preparados para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano.

Se deben definir las responsabilidades para asegurar que se aplique la seguridad a lo largo de todo el tiempo del empleo de la persona dentro de la SSEAF.

4.2.1. Responsabilidad de la SSEAF

La SSEAF solicitará a los empleados, contratistas y usuarios de terceras partes que apliquen la seguridad en concordancia con las políticas y procedimientos establecidos por la organización.

4.3. Cese del empleo o cambio de puesto de trabajo

Objetivo

Asegurar que los usuarios, funcionarios, contratados y terceras personas salgan de la SSEAF o cambien de empleo de una manera ordenada.

Se deben establecer las responsabilidades para asegurar que la salida de la SSEAF de los funcionarios sea manejada y se complete la devolución de todo el equipo y se eliminen todos los derechos de acceso.

4.3.1. Responsabilidad del cese o cambio

Las responsabilidades para realizar la desvinculación o cambio de puesto deben ser claramente definidas y asignadas, incluyendo requerimientos de seguridad y responsabilidades legales a posteriori y, cuando sea apropiado, las responsabilidades contenidas dentro de cualquier acuerdo de confidencialidad, y los términos y condiciones de empleo con continuidad por un período definido de tiempo luego de la finalización del trabajo del empleado, contratista o usuario de tercera parte.

Puede ser necesario informar a los empleados, contratistas y terceros de los cambios en el personal y los acuerdos de operación.

4.3.2. Devolución de Activos

Todos los funcionarios, contratados y usuarios de terceras partes deben devolver todos los activos de la SSEAF en su poder (software, documentos corporativos, equipamiento, dispositivos de computación móviles, tarjetas de crédito, tarjetas de ingreso, etc.) tras la terminación de su empleo, contrato, o acuerdo.

4.3.3. Retiro de los Derechos de Acceso

Se revisarán los derechos de acceso de un individuo a los activos asociados con los sistemas y servicios de información tras la desvinculación, Esto determinará si es necesario remover los derechos de acceso.

Con el cambio de un empleo deben removerse todos los derechos de acceso que no fueron aprobados para el nuevo empleo, comprendiendo esto accesos lógicos y físicos, llaves, tarjetas de identificación, instalaciones de procesamiento de la información, suscripciones, y remoción de cualquier documentación que lo identifique como un miembro corriente de la SSEAF.

Si un funcionario, contratado o usuario de tercera parte que se está desvinculando tiene conocimiento de contraseñas para cuentas que permanecen activas, éstas deben ser cambiadas tras la finalización o cambio de empleo, contrato o acuerdo.

5. Seguridad Física y Ambiental

Generalidades

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones de la SSEAF. Asimismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

Se distinguen tres conceptos a tener en cuenta: la protección física de accesos, la protección ambiental y el transporte, protección y mantenimiento de equipamiento y documentación.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible de la SSEAF, de accesos físicos no autorizados.

El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. Deben contemplarse tanto los riesgos en las instalaciones de la SSEAF como en instalaciones próximas a la sede del mismo que puedan interferir con las actividades.

El equipamiento donde se almacena información es susceptible de mantenimiento periódico, lo cual implica en ocasiones su traslado y permanencia fuera de las áreas protegidas de la SSEAF. Dichos procesos deben ser ejecutados bajo estrictas normas de seguridad y de preservación de la información almacenada en los mismos. Así también se tendrá en cuenta la aplicación de dichas normas en equipamiento perteneciente al Organismo pero situado físicamente fuera del mismo (“housing”) así como en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información al Organismo (“hosting”).

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas mientras no están siendo utilizados. Es por ello que el transporte y la disposición final presentan riesgos que deben ser evaluados.

Gran cantidad de información manejada en las oficinas se encuentra almacenada en papel, por lo que es necesario establecer pautas de seguridad para la conservación de dicha documentación; y para su destrucción cuando así lo amerite.

Objetivo

Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información de la SSEAF.

Proteger el equipamiento de procesamiento de información crítica de la SSEAF ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información de la SSEAF.

Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

Proporcionar protección proporcional a los riesgos identificados.

Alcance

Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información de la SSEAF: instalaciones, equipamiento, cableado, expedientes, medios de almacenamiento, etc.

Responsabilidad

El Departamento de Seguridad de la Información definirá junto con el Director de la DGIC y los Propietarios de Información, según corresponda, las medidas de seguridad 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 seguridad física y ambiental indicadas en el presente Capítulo.

Los Departamentos de Soporte Técnico, Infraestructura de TI, y Comunicaciones de la DGIC asistirán al Departamento de Seguridad de la Información 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 de la SSEAF.

El Director de la DGIC definirá los niveles de acceso físico del personal de la SSEAF a las áreas restringidas bajo su responsabilidad.

Los Propietarios de la Información autorizarán formalmente el trabajo fuera de las instalaciones con información de su incumbencia a los empleados de la SSEAF cuando lo crean conveniente.

El Departamento de Seguridad de la Información revisará los registros de acceso a las áreas protegidas.

Todo el personal de la SSEAF es responsable del cumplimiento de la política de pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario en las oficinas.

Política

5.1. Áreas Seguras

Objetivo

Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la SSEAF.

Los medios de procesamiento de información crítica o confidencial deben ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados. Deben estar físicamente protegidos del acceso no autorizado, daño e interferencia.

5.1.1. Perímetro de seguridad física

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

La SSEAF 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 controlada 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 Director de la DGIC con el asesoramiento del Departamento de Seguridad de la Información, de acuerdo a la evaluación de riesgos efectuada.

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. El acceso a dichas áreas y edificios estará restringido exclusivamente al personal autorizado. Los métodos implementados registrarán cada ingreso y egreso en forma precisa.

a) Extender las barreras físicas necesarias desde el piso hasta el techo, a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo por incendio, humedad e inundación.

b) 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 Departamento de Seguridad de la Información llevará un registro actualizado de los sitios protegidos, indicando:

a) Identificación del Edificio y Área.

b) Principales elementos a proteger.

c) Medidas de protección física.

5.1.2. Controles físicos de entrada

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Departamento de Seguridad de la Información junto con el Director de la DGIC, 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 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 anualmente los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el Responsable de la Unidad Organizativa de la que dependa.

e) Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará el Departamento de Seguridad de la Información.

5.1.3. Seguridad de oficinas, despachos, 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 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 la SSEAF de aquellas administradas por terceros.

g) Restringir el acceso público a los documentos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible.

h) Almacenar los materiales peligrosos o combustibles a una distancia prudencial de las áreas protegidas de la SSEAF. Los suministros, como los útiles de escritorio, no serán trasladados al área protegida hasta que sean requeridos.

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.

5.1.4. Protección contra amenazas externas y de origen ambiental

Se debe asignar y aplicar protección física contra daño por fuego, inundación, derrumbes, 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 debe 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 protegida. Los suministros a granel como papelería no deben almacenarse en el área protegida;
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 contra-incendios ubicado adecuadamente.

5.1.5. Trabajo en áreas seguras

Para incrementar la seguridad de las áreas protegidas, se establecen los siguientes controles y lineamientos adicionales. Esto 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.

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 Responsable de dicha área.

g. Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información.

5.1.6. Áreas de acceso público, de carga y descarga

Se controlarán las áreas de Recepción y Distribución, 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 de la SSEAF, 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.

5.2. Seguridad de los equipos

Objetivo

Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades del Organismo.

Se debe proteger el equipo de amenazas físicas y ambientales.

5.2.1. Ubicación y Protección del Equipamiento

El equipamiento será 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 adecuados para minimizar el riesgo de amenazas potenciales

e. Revisar regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información. Esta revisión se realizará anualmente.

5.2.2. Instalaciones de suministro

El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. 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 de control:

a. Disponer de múltiples tomas o líneas de suministro para evitar un único punto de falla en el suministro de energía.

b. Contar con un suministro de energía ininterrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la SSEAF. La determinación de dichas operaciones críticas, será el resultado del análisis de impacto realizado por el Departamento de Seguridad de la Información, conjuntamente con los Propietarios de la Información 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.

c. Montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Deberá 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 Departamento de Seguridad de la Información conjuntamente con los Propietarios de la Información. 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.

5.2.3. Seguridad del Cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño, mediante las siguientes acciones:

a. Cumplir con los requisitos técnicos vigentes en el país.

b. Utilizar ductos o cableado embutido en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información.

c. Proteger el cableado de red contra intercepción no autorizada o daño.

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.

Para los sistemas sensibles o críticos, se implementarán los siguientes controles adicionales:

a. Instalar ductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección.

b. Utilizar rutas o medios de transmisión alternativos.

5.2.4. Mantenimiento de Equipos

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

a. Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del Director de la DGIC. El Departamento de Soporte Técnico mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.

b. Establecer 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. Registrar el retiro de equipamiento de la sede de la SSEAF para su mantenimiento.

e. Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de respaldo.

5.2.5. Seguridad de los Equipos Fuera de las Instalaciones.

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la SSEAF, será autorizado por el responsable patrimonial. En el caso de que en el mismo se almacene información clasificada, deberá ser aprobado además por el Propietario de la misma. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito de la SSEAF 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 de la SSEAF, cuando sea conveniente.

Los riesgos de seguridad, por ejemplo: daño, robo o intercepción; puede variar considerablemente entre los edificios y se debe tomarlo en cuenta para evaluar los controles apropiados.

5.2.6. Reutilización o retiro seguro de equipos

La información puede verse comprometida por una desafectación o una reutilización descuidada del equipamiento. Los medios de almacenamiento conteniendo material sensible, por ejemplo discos rígidos no removibles, serán físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar, según corresponda.

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

5.2.7. Retirada de materiales propiedad de la empresa

El equipamiento, la información y el software no serán retirados de la sede del Organismo sin autorización formal.

Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos del Organismo. El personal será puesto en conocimiento de la posibilidad de realización de dichas comprobaciones.

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

5.2.8. Políticas de Escritorios y Pantallas Limpias.

Se adopta una 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. 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.

b. Guardar bajo llave la información sensible o crítica de la SSEAF (preferentemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina.

c. Desconectar de los sistemas 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.

d. Proteger los puntos de recepción y envío de correo postal y las máquinas de fax no atendidas.

e. Bloquear las fotocopiadoras (o protegerlas de alguna manera del uso no autorizado) fuera del horario normal de trabajo.

f. Retirar inmediatamente la información sensible o confidencial, una vez impresa.

6. Gestión de Comunicaciones y Operaciones

Generalidades

La proliferación de software malicioso, hace necesario que se adopten medidas de prevención, a efectos de evitar la ocurrencia de tales amenazas.

Es conveniente separar los ambientes de desarrollo, prueba y operaciones de los sistemas de la SSEAF, estableciendo procedimientos que aseguren la calidad de los procesos que se implementen en el ámbito operativo, a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa.

Los sistemas de información están comunicados entre sí, tanto dentro de la SSEAF como con terceros fuera de él. Por lo tanto es necesario establecer criterios de seguridad en las comunicaciones que se establezcan.

Las comunicaciones establecidas permiten el intercambio de información, que deberá estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

Objetivo

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

Alcance

Todas las instalaciones de procesamiento y transmisión de información de la SSEAF.

Responsabilidad

El Departamento de Seguridad de la Información tendrá a su cargo, entre otros:

- Definir procedimientos para el control de cambios a los procesos operativos documentados, los sistemas e instalaciones de procesamiento de información, y verificar su cumplimiento, de manera que no afecten la seguridad de la información.
- Establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas necesarias antes de su aprobación definitiva. Verificar que dichos procedimientos de aprobación de software incluyan aspectos de seguridad.
- Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.
- Definir y documentar una norma clara con respecto al uso del correo electrónico.
- Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados en las redes de la SSEAF.

- Desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.
- Verificar el cumplimiento de las normas, procedimientos y controles establecidos.

Los Departamentos de la DGIC tendrán a su cargo lo siguiente:

- Controlar la existencia de documentación actualizada relacionada con los procedimientos de comunicaciones y operaciones.
- Evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando responsabilidades.
- Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.
- Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario.
- Controlar la realización de las copias de resguardo de información, así como la prueba periódica de su restauración.
- Asegurar el registro de las actividades realizadas por el personal operativo, para su posterior revisión.
- Desarrollar y verificar el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.
- Implementar los controles de seguridad definidos (software malicioso y accesos no autorizados).
- Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento, como cintas, discos, casetes e informes impresos y para la eliminación segura de los mismos.
- Participar en el tratamiento de los incidentes de seguridad, de acuerdo a los procedimientos establecidos.

La DGICE valuará los contratos y acuerdos con terceros para garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados.

Cada Propietario de la Información, con la asistencia del Departamento de Seguridad de la Información y Director de la DGIC, determinará los requerimientos para resguardar la información por la cual es responsable. Asimismo, aprobará los servicios de mensajería autorizados para transportar la información cuando sea requerido, de acuerdo a su nivel de criticidad.

El Departamento de Seguridad de la Información revisará las actividades que no hayan sido posible segregar. Asimismo, revisará los registros de actividades del personal operativo.

Política

6.1. Procedimientos y Responsabilidades Operativas

Objetivo

Asegurar la operación correcta y segura de los medios de procesamiento de la información.

Se deben establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información. Esto incluye el desarrollo de los procedimientos de operación apropiados.

6.1.1. Documentación de los Procedimientos Operativos

Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el Departamento de Seguridad de la Información.

Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

a. Procesamiento y manejo de la información.

b. Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.

c. Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.

d. Restricciones en el uso de utilitarios del sistema.

e. Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.

f. Instrucciones especiales para el manejo de “salidas”, como el uso de papelería especial o la administración de salidas confidenciales, incluyendo procedimientos para la eliminación segura de salidas fallidas de tareas.

g. Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.

Se preparará adicionalmente documentación sobre procedimientos referidos a las siguientes actividades:

a. Instalación y mantenimiento de equipamiento para el procesamiento de información y comunicaciones.

b. Instalación y mantenimiento de las plataformas de procesamiento.

c. Monitoreo del procesamiento y las comunicaciones.

d. Inicio y finalización de la ejecución de los sistemas.

e. Programación y ejecución de procesos.

f. Gestión de servicios.

g. Resguardo de información.

h. Gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones.

i. Remplazo o cambio de componentes del ambiente de procesamiento y comunicaciones.

j. Uso del correo electrónico.

6.1.2. Cambios en las Operaciones

Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.

El Departamento de Seguridad de la Información controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan. Los Departamentos de la DGIC evaluarán el posible impacto operativo de los cambios previstos y verificarán su correcta implementación.

Se retendrá un registro de auditoría que contenga toda la información relevante de cada cambio implementado.

Los procedimientos de control de cambios contemplarán los siguientes puntos:

a. Identificación y registro de cambios significativos.

b. Evaluación del posible impacto de dichos cambios.

c. Aprobación formal de los cambios propuestos.

d. Planificación del proceso de cambio.

e. Prueba del nuevo escenario.

f. Comunicación de detalles de cambios a todas las personas pertinentes.

g. Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

6.1.3. Separación de Funciones

Se separará la gestión o ejecución de ciertas tareas o áreas de responsabilidad, a fin de reducir el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas.

Si este método de control no se pudiera cumplir en algún caso, se implementarán controles como:

a. Monitoreo de las actividades.

b. Registros de auditoría y control periódico de los mismos.

c. Supervisión por parte de un área independiente al área que genera las actividades auditadas.

Asimismo, se documentará la justificación formal por la cual no fue posible efectuar la segregación de funciones.

Se asegurará la independencia de las funciones de auditoría de seguridad, tomando recaudos para que ninguna persona pueda realizar actividades en áreas de responsabilidad única sin ser

monitoreada, y la independencia entre el inicio de un evento y su autorización, considerando los siguientes puntos:

a. Separar actividades que requieren connivencia para defraudar, por ejemplo efectuar una orden de compra y verificar que la mercadería fue recibida.

b. Diseñar controles, si existe peligro de connivencia de manera tal que dos o más personas estén involucradas, reduciendo la posibilidad de conspiración.

6.1.4. Separación entre Instalaciones de Desarrollo e Instalaciones Operativas

Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, estarán separados preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado productivo.

Para ello, se tendrán en cuenta los siguientes controles:

a. Ejecutar el software de desarrollo y de producción, en diferentes ambientes de operaciones, equipos, o directorios.

b. Separar las actividades de desarrollo y prueba, en entornos diferentes.

c. Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente de producción, cuando no sean indispensables para el funcionamiento del mismo.

d. Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Prohibir a los usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.

e. Definir propietarios de la información para cada uno de los ambientes de procesamiento existentes.

f. El personal de desarrollo no tendrá acceso al ambiente de producción. De ser extrema dicha necesidad, se establecerá un procedimiento de emergencia para la autorización, documentación y registro de dichos accesos.

Para el caso que no puedan mantener separados los distintos ambientes en forma física, deberán implementarse los controles indicados en el punto 6.1.3 Separación de Funciones.

6.2. Gestión de Provisión de Servicios

Objetivo

Implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio en línea con los acuerdos de entrega de servicios de terceros.

La SSEAF debe chequear la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados.

6.2.1. Provisión de servicio

Se verificará que los servicios brindados por una tercera parte incluyan los acuerdos de seguridad, definiciones de servicio, y aspectos de la gestión del servicio. En el caso de acuerdos de tercerización, la SSEAF deberá planificar las transiciones necesarias (de la información, de las instalaciones de procesamiento de información, y cualquier otro componente que necesite ser trasladado), y que garantice que la seguridad es mantenida a lo largo del período de transición.

En el caso de tercerizar la administración de las instalaciones de procesamiento, se acordarán controles con el proveedor del servicio y se incluirán en el contrato, contemplando las siguientes cuestiones específicas:

a. Identificar las aplicaciones sensibles o críticas que convenga retener en la DGIC.
b. Obtener la aprobación de los propietarios de aplicaciones específicas.
c. Identificar las implicancias para la continuidad de operaciones de la SSEAF.
d. Especificar las normas de seguridad y el proceso de medición del cumplimiento.
e. Asignar funciones específicas y procedimientos para monitorear todas las actividades de seguridad.
f. Definir las funciones y procedimientos de comunicación y manejo de incidentes relativos a la seguridad.

Dichas consideraciones deben ser determinadas por el Director de la DGIC con la asistencia del Departamento de Seguridad de la Información.

6.2.2. Seguimiento y revisión de los servicios de las terceras partes

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 de seguridad de la información y los problemas son manejados en forma apropiada.

La SSEAF 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. Se recomienda que la organización asegure que se mantenga la visibilidad de las actividades de seguridad como gestión de cambios, identificación de vulnerabilidades y reporte/respuesta de incidentes de seguridad de información a través de un proceso de reportes claro y definido, con formato y estructura.

6.2.3. Gestión del cambio de los servicios de terceras partes

Se gestionarán los cambios en la provisión de los servicios, incluyendo el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los sistemas y procesos del negocio involucrados y la reevaluación de los riesgos.

El proceso de gestión del cambio de un servicio de tercera parte necesita tener en cuenta:

- Los cambios realizados por la SSEAF para implementar:
  - mejoras a los servicios corrientes ofrecidos;

- desarrollo de cualquier aplicación y sistema nuevos;
- modificaciones o actualizaciones de las políticas y procedimientos del Organismo;
- nuevos controles para resolver los incidentes de la seguridad de la información y para mejorar la seguridad;

- Cambios en los servicios de las terceras partes para implementar:
  - cambios y mejoras de las redes;
  - uso de nuevas tecnologías;
  - adopción de nuevos productos o nuevas versiones/publicaciones;
  - nuevas herramientas de desarrollo y ambientes;
  - cambios de las ubicaciones físicas de las instalaciones de servicio;
  - cambio de los vendedores.

6.3. Planificación y Aprobación de Sistemas

Objetivo

Minimizar el riesgo de fallas en los sistemas. Se requiere planificación y preparación anticipadas para asegurar la disponibilidad de la capacidad y los recursos adecuados para entregar el desempeño del sistema requerido.

Se deben realizar proyecciones de los requerimientos de la capacidad futura para reducir el riesgo de sobrecarga en el sistema.

Se deben establecer, documentar y probar los requerimientos operacionales de los sistemas nuevos antes de su aceptación y uso.

6.3.1. Planificación de la Capacidad

Los Departamentos de la DGIC, efectuarán el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados. Para ello tomará en cuenta además los nuevos requerimientos de los sistemas así como las tendencias actuales y proyectadas en el procesamiento de la información de la SSEAF para el período estipulado de vida útil de cada componente. Asimismo, informará las necesidades detectadas a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y puedan planificar una adecuada acción correctiva.

6.3.2. Aprobación del Sistema

Los Departamentos de Sistemas Informáticos y Seguridad de la Información, sugerirán criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva. Se deben considerar los siguientes puntos:

a. Verificar el impacto en el desempeño y los requerimientos de capacidad de las computadoras.

b. Garantizar la recuperación ante errores.

c. Preparar y poner a prueba los procedimientos operativos de rutina según normas definidas.

d. Garantizar la implementación de un conjunto acordado de controles de seguridad.

e. Confeccionar disposiciones relativas a la continuidad de las actividades de la SSEAF.

f. Asegurar que la instalación del nuevo sistema no afectará negativamente los sistemas existentes, especialmente en los períodos de alto requerimiento de procesamiento.

g. Considerar el efecto que tiene el nuevo sistema en la seguridad global de la SSEAF.

h. Disponer la realización de entrenamiento en la operación y/o uso de nuevos sistemas.

6.4. Protección Contra Código Malicioso

Objetivo

Proteger la integridad del software y la integración. Se requiere tomar precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no-autorizados. El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos; como ser, entre otros, virus, troyanos, etc. Los usuarios deben estar al tanto de los peligros de los códigos maliciosos. Cuando sea apropiado, se debe introducir controles para evitar, detectar y eliminar los códigos maliciosos y controlar los códigos móviles.

6.4.1. Código Malicioso

El Departamento de Seguridad de la Información, definirá controles de detección y prevención para la protección contra software malicioso. Los Departamentos de la DGIC implementarán dichos controles.

La DGIC desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

Estos controles deberán considerar las siguientes acciones:

a. Prohibir la instalación y uso de software no autorizado por la SSEAF.

b. Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio (ej.: dispositivos portátiles), señalando las medidas de protección a tomar.

c. Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, como medida precautoria y rutinaria.

d. Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).

e. Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la SSEAF, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas en especial, realizar revisión y análisis de logs.

f. Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.

g. Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.

h. Redactar normas de protección y habilitación de puertos de conexión de dispositivos móviles y sus derechos de acceso.

6.5. Respaldo o Back-up

Objetivo

Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información.
Se deben establecer los procedimientos de rutina para implementar la política de respaldo acordada y la estrategia para realizar copias de respaldo de los datos y practicar su restauración oportuna.

6.5.1. Resguardo de la Información

Los Departamentos de Infraestructura de TI y Seguridad de la Información conjuntamente con los Propietarios de Información determinarán los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá y documentará un esquema de resguardo de la información.

El Departamento de Infraestructura de TI dispondrá y controlará la realización de dichas copias, así como la prueba periódica de su restauración. Para esto se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico de la SSEAF. Los sistemas de resguardo deberán probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades de la SSEAF.

Se definirán procedimientos para el resguardo de la información, que deberán considerar los siguientes puntos:

a. Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.

b. Establecer un esquema de remplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo a lo indicado por el proveedor, y asegurando la destrucción de los medios desechados.

c. Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Se deberán retener al menos tres generaciones o ciclos de

información de resguardo para la información y el software esenciales para la SSEAF. Para la definición de información mínima a ser resguardada en el sitio remoto, se deberá tener en cuenta el nivel de clasificación otorgado a la misma, en términos de y requisitos legales a los que se encuentre sujeta.

d. Asignar a la información de resguardo un nivel de protección física y ambiental según las normas aplicadas en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.

e. Probar periódicamente los medios de resguardo.

f. Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

6.5.2. Registro de Actividades del Personal Operativo

El Responsable del Área Informática asegurará el registro de las actividades realizadas en los sistemas, incluyendo según corresponda:

a. Tiempos de inicio y cierre del sistema.

b. Errores del sistema y medidas correctivas tomadas.

c. Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas.

d. Ejecución de operaciones críticas.

e. Cambios a información crítica.

El responsable de seguridad informática contrastará los registros de actividades del personal operativo con relación a los procedimientos operativos.

6.5.3. Registro de Fallas

El Responsable del Área Informática desarrollará y verificará el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.

Se registrarán las fallas comunicadas, debiendo existir reglas claras para el manejo de las mismas, con inclusión de:

a. Revisión de registros de fallas para garantizar que las mismas fueron resueltas satisfactoriamente.

b. Revisión de medidas correctivas para garantizar que los controles no fueron comprometidos, y que las medidas tomadas fueron autorizadas.

c. Documentación de la falla con el objeto de prevenir su repetición o facilitar su resolución en caso de reincidencia.

d. Integrar la comunicación y gestión de la falla acorde a lo definido en la Política de Gestión de Incidentes de Seguridad.

6.6. Gestión de la Red

Objetivo

Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicancias legales, monitoreo y protección.

También se pueden requerir controles adicionales para proteger la información confidencial que pasa a través de redes públicas.

6.6.1. Redes

El Departamento de Seguridad de la Información definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la SSEAF, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

a. Establecer los procedimientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias, la que será llevada a cabo por el responsable debidamente asignado.

b. Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados. Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas.

c. Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

El Responsable del Área Informática implementará dichos controles.

6.7. Administración y Seguridad de los medios de almacenamiento

Objetivo

Evitar la divulgación no-autorizada; modificación, eliminación o destrucción de activos; y la interrupción de las actividades operativas. Los medios se deberán controlar y proteger físicamente.

Se deben establecer los procedimientos de operación apropiados para proteger los documentos, medios de cómputo (por ejemplo, cintas y discos), entrada/salida de datos (input/output) y documentación del sistema de una divulgación no-autorizada, modificación, eliminación y destrucción.

6.7.1. Administración de Medios Informáticos Removibles

El Departamento de Soporte Técnico, con la asistencia del Departamento de Seguridad de la Información, implementará procedimientos para la administración de medios informáticos removibles, como cintas, discos, pendrives e informes impresos. El cumplimiento de los procedimientos se hará de acuerdo con esta Política.

Se deberán 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 la SSEAF.

b. Requerir autorización para retirar cualquier medio de la SSEAF 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.

Se documentarán todos los procedimientos y niveles de autorización, en concordancia con la Política "Clasificación y Control de Activos".

6.7.2. Eliminación de Medios de Información

El Departamento de Soporte Técnico, junto con el Departamento de Seguridad de la Información definirá procedimientos para la eliminación segura de los medios de información respetando la normativa vigente.

Los procedimientos deberán considerar 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 dispositivos removibles.

h. Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor).

i. Listados de programas.

j. Datos de prueba.

k. Documentación del sistema.

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

6.7.3. Procedimientos de Manejo de la Información

Se definirán procedimientos para el manejo y almacenamiento de la información de acuerdo a la clasificación establecida.

En los procedimientos se contemplarán las siguientes acciones:

a. Incluir en la protección a documentos, sistemas informáticos, redes, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general,

multimedia, servicios e instalaciones postales, uso de máquinas de fax y cualquier otro ítem potencialmente sensible.

b. Restringir el acceso solo al personal debidamente autorizado.

c. Mantener un registro formal de los receptores autorizados de datos.

d. Garantizar que los datos de entrada son completos, que el procesamiento se lleva a cabo correctamente y que se valida las salidas.

e. Proteger los datos en espera ("colas") y memorias temporales (ej.: cache).

f. Conservar los medios de almacenamiento en un ambiente que concuerde con las especificaciones de los fabricantes o proveedores.

6.7.4. Seguridad de la Documentación del Sistema

La documentación del sistema puede contener información sensible, por lo que se considerarán los siguientes recaudos para su protección:

a. Almacenar la documentación del sistema en forma segura.

b. Restringir el acceso a la documentación del sistema al personal estrictamente necesario. Dicho acceso será autorizado por el Propietario de la Información relativa al sistema.

6.8. Intercambios de Información y Software

Objetivo

Mantener la seguridad en el intercambio de información y software dentro de la SSEAF y con cualquier otra entidad externa.

Los intercambios de información y software dentro de las organizaciones se deben basar en una política formal de intercambio, seguida en línea con los acuerdos de intercambio, y en cumplimiento con la legislación vigente.

Se deben establecer los procedimientos y estándares para proteger la información y los medios físicos que contiene la información en tránsito.

6.8.1. Procedimientos y controles de intercambio de la información

Se establecerán procedimientos y controles formales para proteger el intercambio de información a través del uso de todos los tipos de instalaciones de comunicación, considerando lo siguiente:

a. Protección de la información intercambiada de la intercepción, copiado, modificación, de que sea mal dirigida, y de su destrucción

b. detección y protección contra el código malicioso que puede ser transmitido a través del uso de comunicaciones electrónicas

c. definición del uso aceptable de las instalaciones de comunicación electrónicas

d. uso seguro de comunicaciones inalámbricas

e. responsabilidades del empleado, contratista y cualquier otro usuario de no comprometer a la organización, por ejemplo, a través de la difamación, hostigamiento, personificación, reenvío de cadenas de comunicación epistolar, compras no autorizadas y cualquier otro medio (ej.: redes sociales)

f. uso de técnicas criptográficas para proteger la confidencialidad, integridad y la autenticidad de la información

g. directrices de retención y eliminación para toda la correspondencia en concordancia con las leyes y regulaciones relevantes, locales y nacionales

h. instrucción del personal sobre las precauciones que deben tomar a la hora de transmitir información del Organismo.

6.8.2. Acuerdos de Intercambio de Información y Software

Cuando se realicen acuerdos entre organizaciones para el intercambio de información y software, se especificarán el grado de sensibilidad de la información de la SSEAF involucrada y las consideraciones de seguridad sobre la misma. Se tendrán en cuenta los siguientes aspectos:

a. Responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones.

b. Procedimientos de notificación de emisión, transmisión, envío y recepción.

c. Normas técnicas para el empaquetado y la transmisión.

d. Pautas para la identificación del prestador del servicio de correo.

e. Responsabilidades y obligaciones en caso de pérdida, exposición o divulgación no autorizada de datos.

f. Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido y que la información sea adecuadamente protegida.

g. Términos y condiciones de la licencia bajo la cual se suministra el software.

h. Información sobre la propiedad de la información suministrada y las condiciones de su uso.

i. Normas técnicas para la grabación y lectura de la información y del software.

j. Controles especiales que puedan requerirse para proteger ítems sensibles, (claves criptográficas, etc.).

6.8.3. Seguridad de los Medios en Tránsito

Los procedimientos de transporte de medios informáticos entre diferentes puntos (envíos postales y mensajería) deberán contemplar:

a. La utilización de medios de transporte o servicios de mensajería confiables. El Propietario de la Información 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.
2. Entrega en mano.
3. Embalaje a prueba de apertura no autorizada (que revele cualquier intento de acceso).
4. En casos excepcionales, división del objeto a enviar en más de una entrega y envío por diferentes rutas.

6.8.4. Seguridad de la Mensajería

La mensajería electrónica como el correo electrónico, el intercambio de datos electrónicos, la mensajería instantánea y las redes sociales juegan un papel muy importante en las comunicaciones organizacionales. La mensajería electrónica tiene diferentes riesgos que las comunicaciones basadas en papel.

Se considerarán las siguientes medidas de seguridad en los mensajes electrónicos:

- protección de mensajes por el acceso no autorizado, modificaciones o denegación de servicio;

- correcta asignación de la dirección y el transporte del mensaje;

- confiabilidad y disponibilidad general del servicio;

- consideraciones legales, por ejemplo, requerimientos para firmas electrónicas;

- obtención de aprobación previa al uso de los servicios públicos externos tales como mensajería instantánea o el compartir archivos;

- niveles altos de controles de autenticación para los accesos desde las redes públicas

6.9. Seguridad del Correo Electrónico

Objetivo

Garantizar la seguridad de los servicios de correo electrónico y su uso seguro.

Se debieran considerar las implicancias de seguridad asociadas con el uso de servicios de correo electrónico.

6.9.1. Riesgos de Seguridad

Se implementarán controles para reducir los riesgos de incidentes de seguridad en el correo electrónico, contemplando:

a. La vulnerabilidad de los mensajes al acceso o modificación no autorizados o a la negación de servicio.

b. La posible intercepción y el consecuente acceso a los mensajes en los medios de transferencia que intervienen en la distribución de los mismos.

c. Las posibles vulnerabilidades a errores, por ejemplo, consignación incorrecta de la dirección o dirección errónea, y la confiabilidad y disponibilidad general del servicio.

d. La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad de la terminal receptora o de la red a la que se encuentra conectada.

e. El impacto de un cambio en el medio de comunicación en los procesos de la SSEAF.

f. Las consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación.

g. Las implicancias de la publicación externa de información sensible o confidencial, accesibles al público.

h. El acceso de usuarios remotos a las cuentas de correo electrónico.

i. El uso inadecuado por parte del personal.

6.9.2. Política de Correo Electrónico

El Departamento de Seguridad de la Información junto con el Director de la DGIC definirán y documentarán normas y procedimientos claros con respecto al uso del correo electrónico, que incluya al menos los siguientes aspectos:

a. Protección contra ataques al correo electrónico, por ejemplo virus, intercepción, etc.

b. Protección de archivos adjuntos de correo electrónico.

c. Uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos.

d. Retención de mensajes que, si se almacenaran, pudieran ser usados en caso de litigio.

e. Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.

f. Aspectos operativos para garantizar el correcto funcionamiento del servicio (ej.: tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del usuario, etc.).

g. Definición de los alcances del uso del correo electrónico por parte del personal de la SSEAF.

h. Potestad de la SSEAF para auditar los mensajes recibidos o emitidos por los servidores de la SSEAF, lo cual se incluirá en el “Compromiso de Confidencialidad”.

El correo electrónico debe ser entendido a la luz de las normas vigentes que no sólo prohíben a los empleados a hacer uso indebido o con fines particulares del patrimonio estatal sino que

también imponen la obligación de usar los bienes y recursos del estado con los fines autorizados y de manera racional, evitando su abuso, derroche o desaprovechamiento.

El correo electrónico es una herramienta más de trabajo provista al empleado a fin de ser utilizada conforme el uso al cual está destinada, faculta al empleador a implementar sistemas de controles destinados a velar por la protección y el buen uso de sus recursos.

Esta facultad, sin embargo, deberá ejercerse salvaguardando la dignidad del trabajador y su derecho a la intimidad. Por tal motivo, la SSEAF debe informar claramente a sus empleados:

a. cuál es el uso que la SSEAF espera que los empleados hagan del correo electrónico provisto por la SSEAF; y

b. bajo qué condiciones los mensajes pueden ser objeto de control y monitoreo.

6.9.3. Seguridad de los Sistemas Electrónicos de Oficina

Se controlarán los mecanismos de distribución y difusión tales como documentos, computadoras, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios o instalaciones postales, equipos de fax, etc.

Al interconectar dichos medios, se considerarán las implicancias en lo que respecta a la seguridad y a las actividades propias de la SSEAF, incluyendo:

a. Vulnerabilidades de la información en los sistemas de oficina, por ejemplo la grabación de llamadas telefónicas o teleconferencias, la confidencialidad de las llamadas, el almacenamiento de faxes, la apertura o distribución del correo.

b. Procedimientos y controles apropiados para administrar la distribución de información, por ejemplo el uso de boletines electrónicos institucionales.

c. Exclusión de categorías de información sensible de la SSEAF, si el sistema no brinda un adecuado nivel de protección.

d. Limitación del acceso a la información de las actividades que desarrollan determinadas personas, por ejemplo aquellas que trabajan en proyectos sensibles.

e. Categorías de personal y contratistas o terceros a los que se permite el uso del sistema y las ubicaciones desde las cuales se puede acceder al mismo.

f. Restricción de acceso a determinadas instalaciones a específicas categorías de usuarios.

g. Identificación de la posición o categoría de los usuarios, por ejemplo empleados de la SSEAF o contratistas, en directorios accesibles por otros usuarios.

h. Retención y resguardo de la información almacenada en el sistema.

i. Requerimientos y disposiciones relativos a sistemas de soporte de reposición de información previa.

6.9.4. Sistemas de Acceso Público

Se tomarán recaudos para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada que podría dañar la reputación

de la SSEAF. Es posible que la información de un sistema de acceso público, por ejemplo la información en un servidor Web accesible por Internet, deba cumplir con ciertas normas de la jurisdicción en la cual se localiza el sistema o en la cual tiene lugar la transacción electrónica.

Se implementará un proceso de autorización formal antes de que la información se ponga a disposición del público, estableciéndose en todos los casos los encargados de dicha aprobación.

Todos los sistemas de acceso público deberán prever que:

a. La información se obtenga, procese y proporcione de acuerdo a la normativa vigente.

b. La información que se ingresa al sistema de publicación, o aquella que procesa el mismo, sea procesada en forma completa, exacta y oportuna.

c. La información sensible sea protegida durante el proceso de recolección y su almacenamiento.

d. El acceso al sistema de publicación no permita el acceso accidental a las redes a las cuales se conecta el mismo.

e. El responsable de la publicación de información en sistemas de acceso público sea claramente identificado.

f. La información se publique teniendo en cuenta las normas establecidas al respecto.

g. Se garantice la validez y vigencia de la información publicada.

6.9.5. Otras Formas de Intercambio de Información

Se implementarán normas, procedimientos y controles para proteger el intercambio de información a través de medios de comunicaciones de voz, fax y vídeo, contemplando las siguientes acciones:

a. Concientizar al personal sobre la toma de debidas precauciones, por ejemplo no revelar información sensible como para evitar ser escuchado o interceptado, al hacer una llamada telefónica, por:

    1. Personas cercanas, en especial al utilizar teléfonos móviles.

    2. Terceros que tengan acceso a la comunicación mediante la Intervención de la línea telefónica, y otras formas de escucha subrepticias, a través del acceso físico al aparato o a la línea telefónica.

    3. Terceros en el lado receptor.

b. Recordar al personal que no sostengan conversaciones confidenciales en lugares públicos u oficinas abiertas y lugares de reunión con paredes delgadas.

c. No dejar mensajes en contestadores automáticos puesto que éstos pueden ser escuchados por personas no autorizadas, almacenados en sistemas públicos o almacenados incorrectamente como resultado de un error de discado.

d. Recordar al personal los problemas ocasionados por el uso de máquinas de fax, en particular:

1. El acceso no autorizado a sistemas incorporados de almacenamiento de mensajes con el objeto de recuperarlos.
2. La programación deliberada o accidental de equipos para enviar mensajes a determinados números.
3. El envío de documentos y mensajes a un número equivocado por errores de discado o por utilizar el número almacenado equivocado.

6.10. Seguimiento y control

Objetivo

Detectar las actividades de procesamiento de información no autorizadas.

Se deben monitorear los sistemas y se deben reportar los eventos de seguridad de la información. Se deben utilizar bitácoras de operador y se deben registrar las fallas para asegurar que se identifiquen los problemas en los sistemas de información. Una organización debe cumplir con todos los requerimientos legales relevantes aplicables a sus actividades de monitoreo y registro.

Se debe utilizar el monitoreo del sistema para chequear la efectividad de los controles adoptados y para verificar la conformidad con un modelo de política de acceso.

6.10.1. Registro de auditoría

Se producirán y mantendrán registros de auditoría en los cuales se registren las actividades, excepciones, y eventos de seguridad de la información de los usuarios, por un período acordado para permitir la detección e investigación de incidentes.

Se debe evaluar la registración en los mencionados registros de la siguiente información:

a. identificación de los usuarios;
b. fechas, tiempos, y detalles de los eventos principales, por ejemplo, inicio y cierre de sesión;
c. identidad del equipo o la ubicación si es posible;
d. registros de intentos de acceso al sistema exitosos y fallidos;
e. registros de intentos de acceso a los datos u otro recurso, exitosos y rechazados;
f. cambios a 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 que son 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.

6.10.2. Protección de los registros

Se implementarán controles para la protección de los registros de auditoría contra cambios no autorizados y problemas operacionales, incluyendo:

a. alteraciones de los tipos de mensajes que son grabados;

b. edición o eliminación de archivos de registro;

Exceso de la capacidad de almacenamiento de los archivos de registro, resultando en la falla para registrar los eventos o sobrescribiendo eventos registrados en el pasado.

6.10.3. Registro de actividad de administrador y operador

Se registrarán y revisarán periódicamente en particular las actividades de los administradores y operadores de sistema incluyendo:

a. cuenta de administración u operación involucrada;

b. momento en el cual ocurre un evento (éxito o falla);

c. información acerca del evento (por ejemplo, los archivos manipulados) o las fallas (por ejemplo, los errores ocurridos y las acciones correctivas tomadas);

d. procesos involucrados.

6.10.4. Sincronización de Relojes

A fin de garantizar la exactitud de los registros de auditoría, al menos los equipos que realicen estos registros, deben tener una correcta configuración de sus relojes.

Para ello, se dispondrá de un procedimiento de ajuste de relojes, el cual indicará también la verificación de los relojes contra una fuente externa del dato y la modalidad de corrección ante cualquier variación significativa.

7. Gestión de Accesos

Generalidades

El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

Objetivo

Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información. Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

Controlar la seguridad en la conexión entre la red de la SSEAF y otras redes públicas o privadas. Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

Alcance

La Política definida en este documento se aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos o servicios de información de la SSEAF, cualquiera sea la función que desempeñe.

Asimismo se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

Responsabilidad

El Departamento de Seguridad de la Información estará a cargo 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, trabajo remoto y reportes de incidentes relacionados; la respuesta a

la activación de alarmas silenciosas; la revisión de registros de actividades; y el ajuste de relojes de acuerdo a un estándar preestablecido.

- Definir pautas de utilización de Internet para todos los usuarios.
- Participar en la definición de normas y procedimientos de seguridad a implementar en el ambiente informático (ej.: sistemas operativos, servicios de red, enrutadores o gateways, etc.) y validarlos periódicamente.
- Controlar periódicamente la asignación de privilegios a usuarios.
- Analizar y sugerir medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registración de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios y nodos, uso controlado de utilitarios del sistema, alarmas silenciosas, desconexión de terminales por tiempo muerto, limitación del horario de conexión, registro de eventos, protección de puertos (físicos y lógicos), subdivisión de redes, control de conexiones a la red, control de ruteo de red, etc.
- Concientizar a los usuarios sobre el uso apropiado de contraseñas y de equipos de trabajo.
- Verificar el cumplimiento de los procedimientos de revisión de registros de auditoría.
- Asistir a los usuarios que corresponda en el análisis de riesgos a los que se expone la información y los componentes del ambiente informático que sirven de soporte a la misma.

Los Propietarios de la Información estarán encargados de:

- Evaluar los riesgos a los cuales se expone la información con el objeto de:
    - determinar los controles de accesos, autenticación y utilización a ser implementados en cada caso.
    - definir los eventos y actividades de usuarios a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de revisión de los mismos.
- Aprobar y solicitar la asignación de privilegios a usuarios.
- Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso a la información.

Los Directores de la SSEAF, junto con el Departamento de Seguridad de la Información autorizarán el trabajo remoto 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 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.

El Director de la DGIC cumplirá las siguientes funciones:

- Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.

- Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.
- Evaluar el costo y el impacto de la implementación de "enrutadores" o "gateways" adecuados para subdividir la red y recomendar el esquema apropiado.
- Implementar el control de puertos, de conexión a la red y de ruteo de red.
- Implementar el registro de eventos o actividades de usuarios de acuerdo a lo definido por los propietarios de la información, así como la depuración de los mismos.
- Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento.
- Evaluar los riesgos sobre la utilización de las instalaciones de procesamiento de información, con el objeto de definir medios de monitoreo y tecnologías de identificación y autenticación de usuarios (Ej.: biometría, verificación de firma, uso de autenticadores de hardware).
- Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera de garantizar la seguridad en su operatoria.
- Analizar las medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Otorgar acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal correspondiente.
- Efectuar un control de los registros de auditoría generados por los sistemas operativos y de comunicaciones.

El Departamento de Seguridad de la Información tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

Política

7.1. Requerimientos para el Control de Acceso

Objetivo

Controlar el acceso a la información. Se debe controlar el acceso a la información, medios de procesamiento de la información y procesos de negocio sobre la base de los requerimientos de negocio y de seguridad.

Las reglas de control de acceso deben tomar en cuenta las políticas para la divulgación y autorización de la información.

7.1.1. Política de Control de Accesos

En la aplicación de controles 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 y redes.

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 y de red, que reconozcan todos los tipos de conexiones disponibles.

7.1.2. Reglas de Control de Acceso

Las reglas de control de acceso especificadas, deberán:

a. Indicar expresamente si las reglas son obligatorias u optativas.

b. Establecer reglas sobre la premisa “Todo debe estar prohibido a menos que se permita expresamente” y no sobre la premisa inversa de “Todo está permitido a menos que se prohíba expresamente”.

c. Controlar los cambios en los rótulos de información que son iniciados automáticamente por herramientas de procesamiento de información, de aquellos que son iniciados a discreción del usuario.

d. Controlar los cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos que son iniciados por el administrador.

e. Controlar las reglas que requieren la aprobación del administrador o del Propietario de la Información de que se trate, antes de entrar en vigencia, y aquellas que no requieren aprobación.

7.2. Administración de Accesos de Usuarios

Objetivo

Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

Los procedimientos debieran abarcar todas las etapas en el ciclo de vida del acceso del usuario, desde el registro inicial de usuarios nuevos hasta la baja final de los usuarios que ya no requieren acceso a los sistemas y servicios de información.

7.2.1. Registración de Usuarios

El Departamento de Seguridad de la Información, 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 Propietario de la Información 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 Política de Seguridad de la SSEAF, 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.

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 de la SSEAF o sufrieron la pérdida/robo de sus credenciales de acceso.

i. Efectuar revisiones periódicas con el objeto de:

   - cancelar identificadores y cuentas de usuario redundantes
   - eliminar o inhabilitar cuentas inactivas

   En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.

j. Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.

k. 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.

7.2.2. Gestión de Privilegios

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.

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

Los Propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el Departamento de Seguridad de la Información.

7.2.3. Gestión de Contraseñas de Usuario

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 provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez acreditada la identidad del usuario.

c. Generar contraseñas provisorias 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 Departamento de Seguridad de la Información conjuntamente con el Director de la DGIC y el Propietario de la Información lo determine necesario (o lo justifique).

f. Configurar los sistemas de tal manera que cumplan con las reglas definidas en materia de:

- longitud mínima de las contraseñas,
- cantidad máxima de intentos de entrar con una contraseña incorrecta antes de la suspensión o bloqueo del usuario (deberá pedir la rehabilitación ante quien corresponda),
- cantidad máxima de días de vigencia de la contraseña,

- cantidad de las últimas contraseñas que no podrán ser reutilizadas,
- tiempo de vida mínimo para las nuevas contraseñas.

7.2.4. Administración de Contraseñas Críticas

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 Departamento de Seguridad de la Información 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 Departamento de Seguridad de la Información.

7.2.5. Revisión de Derechos de Acceso de Usuarios

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Propietario de la Información de que se trate llevará a cabo un proceso formal, a intervalos regulares, a fin de revisar los derechos de acceso de los usuarios. Se deberán contemplar los siguientes controles:

a. Revisar los derechos de acceso de los usuarios con la periodicidad establecida.

b. Revisar las autorizaciones de privilegios especiales de derechos de acceso con la periodicidad establecida.

c. Revisar las asignaciones de privilegios con la periodicidad establecida, a fin de garantizar que no se obtengan privilegios no autorizados.

7.3. Responsabilidades del Usuario

Objetivo

Evitar el acceso de usuarios no-autorizados, evitar poner en peligro la información y evitar el robo de información y los medios de procesamiento de la información.

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.

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.

7.3.1. Uso de Contraseñas

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 Responsable del Activo de Información 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 contraseñas anteriores.

e. Cambiar las contraseñas provisorias en el primer inicio de sesión.

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

7.3.2. Equipos Desatendidos en Áreas de Usuarios

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente.

Los equipos instalados en áreas de usuarios, por ejemplo estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

Se debe concientizar a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección.

Los usuarios cumplirán con las siguientes pautas:

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.

7.4. Control de Acceso a la Red

Objetivo

Evitar el acceso no autorizado a los servicios de la red.

Se debe controlar el acceso a los servicios de redes internas y externas.

El acceso del usuario a las redes y servicios de las redes no deben comprometer la seguridad de los servicios de la red asegurando:

a. que existan las interfaces apropiadas entre la red de la SSEAF y las redes de otras organizaciones, y redes públicas;
b. se apliquen los mecanismos de autenticación apropiados para los usuarios y el equipo;
c. el control del acceso del usuario a la información sea obligatorio.

7.4.1. Política de Utilización de los Servicios de Red

Las conexiones no seguras a los servicios de red pueden afectar a toda la SSEAF, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

El Director de la DGIC tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal de la Dirección de la SSEAF que lo solicite para personal de su incumbencia.

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo áreas públicas o externas que están fuera de la administración y del control de seguridad de la SSEAF.

Para ello, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

a. Identificar las redes y servicios de red a los cuales se permite el acceso.

b. Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.

c. Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

Esta Política será coherente con la Política de Control de Accesos de la SSEAF.

7.4.2. Camino Forzado

Las redes están diseñadas para permitir el máximo alcance de distribución de recursos y flexibilidad en la elección de la ruta a utilizar. Estas características también pueden ofrecer oportunidades para el acceso no autorizado a las aplicaciones de la SSEAF, o para el uso no autorizado de servicios de información. Por esto, el camino de las comunicaciones será controlado.

Se limitarán las opciones de elección de la ruta entre la terminal de usuario y los servicios a los cuales el mismo se encuentra autorizado a acceder, mediante la implementación de controles en diferentes puntos de la misma.

A continuación se enumeran algunos ejemplos a considerar en caso de implementar estos controles a los sistemas existentes:

a. Asignar números telefónicos o líneas, en forma dedicada.

b. Establecer la conexión automática de puertos a gateways de seguridad o a sistemas de aplicación específicos.

c. Limitar las opciones de menú y submenú de cada uno de los usuarios.

d. Evitar la navegación ilimitada por la red.

e. Imponer el uso de sistemas de aplicación y/o gateways de seguridad específicos para usuarios externos de la red.

f. Controlar activamente las comunicaciones con origen y destino autorizados a través de un gateway, por ejemplo utilizando firewalls y generando alertas ante eventos no previstos.

g. Restringir el acceso a redes, estableciendo dominios lógicos separados, por ejemplo, redes privadas virtuales para grupos de usuarios dentro o fuera de la SSEAF.

Los requerimientos relativos a caminos forzados se basarán en la Política de Control de Accesos de la SSEAF. El Departamento de Seguridad de la Información, conjuntamente con el Propietario de la Información de que se trate, realizará una evaluación de riesgos a fin de determinar los mecanismos de control que corresponda en cada caso.

7.4.3. Autenticación de Usuarios para Conexiones Externas

Las conexiones externas son de gran potencial para accesos no autorizados a la información de la SSEAF. Por consiguiente, el acceso de usuarios remotos estará sujeto al cumplimiento de

procedimientos de autenticación. Existen diferentes métodos de autenticación, algunos de los cuales brindan un mayor nivel de protección que otros. El Departamento de Seguridad de la Información, conjuntamente con el Propietario de la Información de que se trate, realizará una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

La autenticación de usuarios remotos puede llevarse a cabo utilizando:

a. Un método de autenticación físico (por ejemplo tokens de hardware), para lo que debe implementarse un procedimiento que incluya:
   - Asignación de la herramienta de autenticación.
   - Registro de los poseedores de autenticadores.
   - Mecanismo de rescate al momento de la desvinculación del personal al que se le otorgó.
   - Método de revocación de acceso del autenticador, en caso de compromiso de seguridad.
b. Un protocolo de autenticación (por ejemplo desafío / respuesta), para lo que debe implementarse un procedimiento que incluya:
   - Establecimiento de las reglas con el usuario.
   - Establecimiento de un ciclo de vida de las reglas para su renovación.
c. También pueden utilizarse líneas dedicadas privadas o una herramienta de verificación de la dirección del usuario de red, a fin de constatar el origen de la conexión.

7.4.4. Autenticación de Nodos

Una herramienta de conexión automática a una computadora remota podría brindar un medio para obtener acceso no autorizado a una aplicación de la SSEAF. Por consiguiente, las conexiones a sistemas informáticos remotos serán autenticadas. Esto es particularmente importante si la conexión utiliza una red que está fuera de control de la gestión de seguridad de la SSEAF. En el punto anterior se mencionan algunos ejemplos de autenticación y de cómo puede lograrse. La autenticación de nodos puede servir como un medio alternativo de autenticación de grupos de usuarios remotos, cuando éstos están conectados a un servicio informático seguro y compartido.

7.4.5. Protección de los Puertos (Ports) de Diagnóstico Remoto

Muchas computadoras y sistemas de comunicación son instalados y administrados con una herramienta de diagnóstico remoto. Si no están protegidos, estos puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado, con las mismas características del punto “Autenticación de Usuarios para Conexiones Externas”. También para este caso deberá tenerse en cuenta el punto “Camino Forzado”.

7.4.6. Subdivisión de Redes

Para controlar la seguridad en redes extensas, se podrán dividir en dominios lógicos separados. Para esto se definirán y documentarán los perímetros de seguridad que sean convenientes. Estos perímetros se implementarán mediante la instalación de "gateways" con funcionalidades de "firewall" o redes privadas virtuales, para filtrar el tráfico entre los dominios y para bloquear el acceso no autorizado de acuerdo a la Política de Control de Accesos.

La subdivisión en dominios de la red tomará en cuenta criterios como los requerimientos de seguridad comunes de grupos de integrantes de la red, la mayor exposición de un grupo a peligros externos, separación física, u otros criterios de aglutinamiento o segregación preexistentes.

Basándose en la Política de Control de Accesos y los requerimientos de acceso, el Director de la DGIC evaluará el costo relativo y el impacto en el desempeño que ocasione la implementación de enrutadores o gateways adecuados para subdividir la red. Luego decidirá, junto con el Departamento de Seguridad de la Información, el esquema más apropiado a implementar.

7.4.7. Acceso a Internet

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto.

El Departamento de Seguridad de la Información definirá procedimientos para solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente por las Direcciones del personal que lo solicite. Asimismo, se definirán las pautas de utilización de Internet para todos los usuarios.

Se evaluará la conveniencia de generar un registro de los accesos de los usuarios a Internet, con el objeto de realizar revisiones de los accesos efectuados o analizar casos particulares. Dicho control será comunicado a los usuarios de acuerdo a lo establecido en el punto "Compromiso de Confidencialidad". Para ello, el Departamento de Seguridad de la Información junto con el Director de la DGIC analizarán las medidas a ser implementadas para efectivizar dicho control, como ser la instalación de "firewalls", "proxies", etc.

7.4.8. Conexión a la Red

Sobre la base de lo definido en el punto "Requerimientos de Control de Accesos", se implementarán controles para limitar la capacidad de conexión de los usuarios. Dichos controles se podrán implementar en los "gateways" que separen los diferentes dominios de la red.

Algunos ejemplos de los entornos a las que deben implementarse restricciones son:

a. Correo electrónico.

b. Transferencia de archivos.

c. Acceso interactivo.

d. Acceso a la red fuera del horario laboral.

7.4.9. Ruteo de Red

En las redes compartidas, especialmente aquellas que se extienden fuera de los límites de la SSEAF, se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos. Estos controles contemplarán

mínimamente la verificación positiva de direcciones de origen y destino. Adicionalmente, para este objetivo pueden utilizarse diversos métodos incluyendo, entre otros, autenticación de protocolos de ruteo, ruteo estático, traducción de direcciones y listas de control de acceso.

7.4.10. Seguridad de los Servicios de Red

El Departamento de Seguridad de la Información junto con el Director de la DGIC definirá las pautas para garantizar la seguridad de los servicios de red de la SSEAF, tanto públicos como privados.

Para ello se tendrán en cuenta las siguientes directivas:

- Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
- Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.
- Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.
- Instalar periódicamente las actualizaciones de seguridad.

Dicha configuración será revisada periódicamente por el Departamento de Seguridad de la Información.

7.5. Control de Acceso al Sistema Operativo

Objetivo

Evitar el acceso no autorizado a los sistemas operativos.

Se deben utilizar medios de seguridad para restringir el acceso a los sistemas operativos a los usuarios autorizados. Los medios deben tener la capacidad para:

a. autenticar a los usuarios autorizados, en concordancia con una política de control de acceso definida;
b. registrar los intentos exitosos y fallidos de autenticación del sistema;
c. registrar el uso de los privilegios especiales del sistema;
d. emitir alarmas cuando se violan las políticas de seguridad del sistema;
e. proporcionar los medios de autenticación apropiados;
f. cuando sea apropiado, restringir el tiempo de conexión de los usuarios.

7.5.1. Identificación Automática de Terminales

El Departamento de Seguridad de la Información junto con el Departamento de Infraestructura realizará una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo.

Si del análisis realizado surgiera la necesidad de proveer un método de identificación de terminales, se redactará un procedimiento que indique:

a. El método de identificación automática de terminales utilizado.

b. El detalle de transacciones permitidas por terminal.

7.5.2. Procedimientos de Conexión de Terminales

El acceso a los servicios de información sólo será posible a través de un proceso de conexión seguro. El procedimiento de conexión en un sistema informático será diseñado para minimizar la oportunidad de acceso no autorizado.

Este procedimiento, por lo tanto, debe divulgar la mínima información posible acerca del sistema, a fin de evitar proveer de asistencia innecesaria a un usuario no autorizado.

El procedimiento de identificación deberá:

a. Mantener en secreto los identificadores de sistemas o aplicaciones hasta tanto se haya llevado a cabo exitosamente el proceso de conexión.

b. Desplegar un aviso general advirtiendo que sólo los usuarios autorizados pueden acceder a la computadora.

c. Evitar dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión.

d. Validar la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surge una condición de error, el sistema no debe indicar que parte de los datos es correcta o incorrecta.

e. Limitar el número de intentos de conexión no exitosos permitidos y:

   - Registrar los intentos no exitosos.
   - Impedir otros intentos de identificación, una vez superado el límite permitido.
   - Desconectar conexiones de comunicaciones de datos.

f. Limitar el tiempo máximo permitido para el procedimiento de conexión. Si este es excedido, el sistema debe finalizar la conexión.

g. Desplegar la siguiente información, al completarse una conexión exitosa:

   - Fecha y hora de la conexión exitosa anterior.
   - Detalles de los intentos de conexión no exitosos desde la última conexión exitosa.

7.5.3. Identificación y Autenticación de los Usuarios

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

En circunstancias excepcionales, cuando existe un claro beneficio para la SSEAF, podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea específica. Para casos de esta índole, se documentará la justificación y aprobación del Propietario de la Información de que se trate.

Si se utilizará un método de autenticación físico (por ejemplo autenticadores de hardware), deberá implementarse un procedimiento que incluya:

a. Asignar la herramienta de autenticación.

b. Registrar los poseedores de autenticadores.

c. Rescatar el autenticador al momento de la desvinculación del personal al que se le otorgó.

d. Revocar el acceso del autenticador, en caso de compromiso de seguridad.

7.5.4. Sistema de Administración de Contraseñas

Las contraseñas constituyen uno de los principales medios de validación de la autoridad de un usuario para acceder a un servicio informático. Los sistemas de administración de contraseñas deben constituir una herramienta eficaz e interactiva que garantice contraseñas de calidad.

El sistema de administración de contraseñas debe:

a. Imponer el uso de contraseñas individuales para determinar responsabilidades.

b. Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de las mismas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso.

c. Imponer una selección de contraseñas de calidad según lo señalado en la Política.

d. Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en la Política.

e. Obligar a los usuarios a cambiar las contraseñas provisorias en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.

f. Mantener un registro de las últimas contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.

g. Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.

h. Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.

i. Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.

j. Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware.

k. Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, asegure que no se tenga acceso a información temporal o en tránsito de forma no protegida.

7.5.5. Uso de Utilitarios de Sistema

La mayoría de las instalaciones informáticas tienen uno o más programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Es esencial

que su uso sea limitado y minuciosamente controlado. Se deben considerar los siguientes controles:

a. Utilizar procedimientos de autenticación para utilitarios del sistema.

b. Separar entre utilitarios del sistema y software de aplicaciones.

c. Limitar el uso de utilitarios del sistema a la cantidad mínima viable de usuarios fiables y autorizados.

d. Evitar que personas ajenas a la SSEAF tomen conocimiento de la existencia y modo de uso de los utilitarios instalados en las instalaciones informáticas.

e. Establecer autorizaciones para uso ad hoc de utilitarios de sistema.

f. Limitar la disponibilidad de utilitarios de sistema, por ejemplo durante el transcurso de un cambio autorizado.

g. Registrar todo uso de utilitarios del sistema.

h. Definir y documentar los niveles de autorización para utilitarios del sistema.

i. Remover todo el software basado en utilitarios y software de sistema innecesarios.

7.5.6. Desconexión de Terminales por Tiempo Muerto

El Departamento de Seguridad de la Información, junto con los Propietarios de la Información de que se trate, definirán cuáles se consideran terminales de alto riesgo, por ejemplo áreas públicas o externas fuera del alcance de la gestión de seguridad de la SSEAF, o que sirven a sistemas de alto riesgo. Las mismas se apagarán después de un periodo definido de inactividad (tiempo muerto) para evitar el acceso de personas no autorizadas. Esta herramienta de desconexión por tiempo muerto deberá limpiar la pantalla de la terminal y deberá cerrar tanto la sesión de la aplicación como la de red. El lapso por tiempo muerto responderá a los riesgos de seguridad del área y de la información que maneje la terminal.

Para las estaciones de trabajo, se implementará la desconexión por tiempo muerto, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red.

Por otro lado, si la persona debe abandonar su puesto de trabajo momentáneamente, activará protectores de pantalla con contraseñas, a los efectos de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

7.5.7. Limitación del Horario de Conexión

Las restricciones al horario de conexión deben suministrar seguridad adicional a las aplicaciones de alto riesgo. La limitación del periodo durante el cual se permiten las conexiones de terminales a los servicios informáticos reduce el espectro de oportunidades para el acceso no autorizado. Se implementará un control de esta índole para aplicaciones informáticas sensibles, especialmente aquellas terminales instaladas en ubicaciones de alto riesgo, por ejemplo áreas públicas o externas que estén fuera del alcance de la gestión de seguridad de la SSEAF.

Entre los controles que se deben aplicar, se enuncian:

a. Utilizar lapsos predeterminados, por ejemplo para transmisiones de archivos en lote, o sesiones interactivas periódicas de corta duración.

b. Limitar los tiempos de conexión al horario normal de oficina, de no existir un requerimiento operativo de horas extras o extensión horaria.

c. Documentar debidamente las personas que no tienen restricciones horarias y las razones de su autorización. También cuando el Propietario de la Información autorice excepciones para una extensión horaria ocasional.

7.6. Control de Acceso a las Aplicaciones

Objetivo

Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.

Se deben utilizar medios de seguridad para restringir el acceso a y dentro de los sistemas de aplicación.

El acceso lógico al software de la aplicación y la información se debe limitar a los usuarios autorizados. Los sistemas de aplicación debieran:

a. controlar el acceso del usuario a la información y las funciones del sistema de aplicación, en concordancia con una política de control de acceso definida;
b. proporcionar protección contra un acceso no autorizado de cualquier utilidad, software del sistema de operación y software malicioso que sea capaz de superar o pasar los controles del sistema o la aplicación;
c. no comprometer a otros sistemas con los cuales se comparten recursos de información.

7.6.1. Restricción del Acceso a la Información

Los usuarios de sistemas de aplicación, con inclusión del personal de soporte, tendrán acceso a la información y a las funciones de los sistemas de aplicación de conformidad con la Política de Control de Acceso definida, sobre la base de los requerimientos de cada aplicación, y conforme a la Política de la SSEAF para el acceso a la información.

Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

a. Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación. El Propietario de la Información involucrada será responsable de la adjudicación de accesos a las funciones. En el caso de que las actividades involucradas en el otorgamiento de acceso revistan un carácter técnico elevado, las mismas serán llevadas a cabo por personal del área de TI, conforme a una autorización formal emitida por el Propietario de la Información.

b. Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizados a acceder, con la adecuada edición de la documentación de usuario.

c. Controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.

d. Garantizar que las salidas de los sistemas de aplicación que administran información sensible, contengan sólo la información que resulte pertinente para el uso de la salida, y que la misma se envíe solamente a las terminales y ubicaciones autorizadas.

e. Revisar periódicamente dichas salidas a fin de garantizar la remoción de la información redundante.

f. Restringir el acceso a la información por fuera del sistema encargado de su procesamiento, es decir, la modificación directa del dato almacenado.

7.6.2. Aislamiento de los Sistemas Sensibles

Los sistemas críticos podrían requerir de un ambiente informático dedicado (aislado). Algunos sistemas de aplicación son suficientemente sensibles a pérdidas potenciales y requieren un tratamiento especial. La sensibilidad puede señalar que el sistema de aplicación debe ejecutarse en una computadora dedicada, que sólo debe compartir recursos con los sistemas de aplicación confiables, o no tener limitaciones. Son aplicables las siguientes consideraciones:

a. Identificar y documentar claramente la sensibilidad de un sistema de aplicación. Esta tarea será llevada a cabo por el administrador de la aplicación (conforme a la Clasificación y Control de Activos).

b. Identificar y acordar con el administrador de la aplicación sensible cuando la aplicación ha de ejecutarse en un ambiente compartido, los sistemas de aplicación con los cuales ésta compartirá los recursos.

c. Coordinar con el Responsable del Área informática, qué servicios estarán disponibles en el entorno donde se ejecutará la aplicación, de acuerdo a los requerimientos de operación y seguridad especificados por el administrador de la aplicación.

d. Considerar la seguridad en la administración de las copias de respaldo de la información que procesan las aplicaciones.

e. Considerar las mismas precauciones de seguridad y privacidad, en la elaboración del plan de continuidad y/o contingencia de la ejecución de la aplicación. Ejemplo: el equipamiento alternativo o las instalaciones de emergencia donde restablecer la aplicación.

7.7. Monitoreo del Acceso y Uso de los Sistemas

Objetivo

Asegurar que se registren y se evalúen todos los eventos significativos para la seguridad de accesos.

Verificar la existencia de procedimientos para monitorear el uso de las instalaciones de procesamiento de la información.

7.7.1. Registro de Eventos

Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad.

Los registros de auditoría deberán incluir:

a. Identificación del usuario.

b. Fecha y hora de inicio y terminación.

c. Identidad o ubicación de la terminal, si se hubiera dispuesto identificación automática para la misma.

d. Registros de intentos exitosos y fallidos de acceso al sistema.

e. Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

En todos los casos, los registros de auditoría serán archivados preferentemente en un equipo diferente al que los genere y conforme los requerimientos de la Política de Retención de Registros.

Los Propietarios de la Información junto con el Departamento de Seguridad de la Información definirán un cronograma de depuración de registros en línea en función a normas vigentes y a sus propias necesidades.

7.7.2. Procedimientos y Áreas de Riesgo

Se desarrollarán procedimientos para monitorear el uso de las instalaciones de procesamiento de la información, a fin de garantizar que los usuarios sólo estén desempeñando actividades que hayan sido autorizadas explícitamente.

Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos, y se les advertirá que determinadas actividades pueden ser objeto de control y monitoreo.

El alcance de estos procedimientos deberá corresponderse a la evaluación de riesgos que realicen los Departamentos de la DGIC con la asistencia del Departamento de Seguridad de la Información.

Entre las áreas que deben tenerse en cuenta se enumeran las siguientes:

a. Acceso no autorizado, incluyendo detalles como:

    1. Identificación del usuario.

    2. Fecha y hora de eventos clave.

    3. Tipos de eventos.

    4. Archivos a los que se accede.

    5. Utilitarios y programas utilizados.

b. Todas las operaciones con privilegio, como:

1. Utilización de cuenta de supervisor.
2. Inicio y cierre del sistema.
3. Conexión y desconexión de dispositivos de Ingreso y Salida de información o que permitan copiar datos.
4. Cambio de fecha/hora.
5. Cambios en la configuración de la seguridad.
6. Alta de servicios.

c. Intentos de acceso no autorizado, como:

1. Intentos fallidos.
2. Violaciones de la Política de Accesos y notificaciones para “gateways” de red y “firewalls”.
3. Alertas de sistemas de detección de intrusiones.

d. Alertas o fallas de sistema como:

1. Alertas o mensajes de consola.
2. Excepciones del sistema de registro.
3. Alarmas del sistema de administración de redes.
4. Accesos remotos a los sistemas.

Entre los factores de riesgo que se deben considerar se encuentran:

a. La criticidad de los procesos de aplicaciones.

b. El valor, la sensibilidad o criticidad de la información involucrada.

c. La experiencia acumulada en materia de infiltración y uso inadecuado del sistema.

d. El alcance de la interconexión del sistema (en particular las redes públicas).

Los Propietarios de la Información manifestarán la necesidad de registrar aquellos eventos que consideren críticos para la operatoria que se encuentra bajo su responsabilidad.

7.7.3. Registro y Revisión de Eventos

Se implementará un procedimiento de registro y revisión de los registros de auditoría, orientado a producir un informe de las amenazas detectadas contra los sistemas y los métodos utilizados. La periodicidad de dichas revisiones será definida por los Propietarios de la Información y el Departamento de Seguridad de la Información, de acuerdo a la evaluación de riesgos efectuada.

Si el volumen de la información contenida en alguno de los registros fuera muy grande, el procedimiento indicará cuales de los registros más significativos se copiarán automáticamente en registros auxiliares.

Por otra parte, el Director de la DGIC, podrá disponer la utilización de herramientas de auditoría o utilitarios adecuados para llevar a cabo el control de los registros.

En la asignación de funciones en materia de seguridad de la información, se deberá separar las funciones entre quienes realizan la revisión y aquellos cuyas actividades están siendo monitoreadas.

Las herramientas de registro deberán contar con los controles de acceso necesarios, a fin de garantizar que no ocurra:

a. La desactivación de la herramienta de registro.

b. La alteración de mensajes registrados.

c. La edición o supresión de archivos de registro.

d. La saturación de un medio de soporte de archivos de registro.

e. La falla en los registros de los eventos.

f. La sobre escritura de los registros.

El área de Seguridad de la Información, tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

7.8. Dispositivos Móviles y Trabajo Remoto

Objetivo

Asegurar la información cuando se utiliza medios de computación y tele-trabajo móviles.

La protección requerida debe ser adecuada con los riesgos que causan estas maneras de trabajo específicas. Cuando se utiliza computación móvil, se deben considerar los riesgos de trabajar en un ambiente desprotegido y se debiera aplicar la protección apropiada. En el caso del tele-trabajo, la organización debe aplicar protección al lugar del tele-trabajo y asegurar que se establezcan los mecanismos adecuados para esta manera de trabajar.

7.8.1. Computación Móvil

Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información de la SSEAF.

Se deberá tener en cuenta en este sentido, cualquier dispositivo móvil y/o removible, incluyendo: Notebooks, Laptop o PDA (Asistente Personal Digital), Teléfonos Celulares y sus tarjetas de memoria, Dispositivos de Almacenamiento removibles, tales como CDs, DVDs, Disquetes, 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 deberán incluirse todos los dispositivos que pudieran contener información confidencial de la SSEAF 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.

c. La utilización de los dispositivos en lugares públicos.

d. El acceso a los sistemas de información y servicios de la SSEAF 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 deberá entrenarse especialmente al personal que los utilice. Se desarrollarán normas y 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 de la SSEAF en el dispositivo, salvo los estrictamente necesarios.

e. No poner datos de contacto técnico en el dispositivo.

f. Mantener cifrada la información clasificada.

Por otra parte, se confeccionarán procedimientos que permitan al propietario del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información de la SSEAF, los que incluirán:

a. Revocación de las credenciales afectadas.

b. Notificación a grupos de Trabajo donde potencialmente se pudieran haber comprometido recursos.

7.8.2. Trabajo Remoto

El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar externo a la SSEAF.

El trabajo remoto sólo será autorizado por el Director de la DGIC, conjuntamente con el Departamento de Seguridad de la Información, cuando se verifique 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 de excepción y serán contemplados en situaciones que justifiquen la imposibilidad de otra forma de acceso y la urgencia, tales como horarios de la SSEAF, solicitud de las autoridades, etc.

Para ello, se establecerán normas y procedimientos para el trabajo remoto, que consideren los siguientes aspectos:

a. La seguridad física existente en el sitio de trabajo remoto, tomando en cuenta la seguridad física del edificio y del ambiente local.

b. El ambiente de trabajo remoto propuesto.

c. Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos de la SSEAF, 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.

d. La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, por ejemplo, familia y amigos.

e. Evitar la instalación / desinstalación de software no autorizada por la SSEAF.

Los controles y disposiciones comprenden:

a. Proveer de mobiliario para almacenamiento y equipamiento adecuado para las actividades de trabajo remoto.

b. Definir el trabajo permitido, el horario de trabajo, la clasificación de la información que se puede almacenar en el equipo remoto desde el cual se accede a la red de la SSEAF y los sistemas internos y servicio a los cuales el trabajador remoto está autorizado a acceder.

c. Proveer de un adecuado equipo de comunicación, con inclusión de métodos para asegurar el acceso remoto.

d. Incluir seguridad física.

e. Definir reglas y orientación respecto del acceso de terceros al equipamiento e información.

f. Proveer el hardware y el soporte y mantenimiento del software.

g. Definir los procedimientos de backup y de continuidad de las operaciones.

h. Efectuar auditoría y monitoreo de la seguridad.

i. Realizar la anulación de las autorizaciones, derechos de acceso y devolución del equipo cuando finalicen las actividades remotas.

j. 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.

8. Desarrollo y Mantenimiento de Sistemas

Generalidades

El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad.

Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deberán diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.

Dado que los analistas y programadores tienen el conocimiento total de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas, bases de datos y plataformas de software de base (por ejemplo, operadores que puedan manipular los datos y/o atacantes que puedan comprometer/alterar la integridad de las bases de datos) y en el caso de que se lleven a cabo, identificar rápidamente al responsable.

Asimismo, es necesaria una adecuada administración de la infraestructura de base, Sistemas Operativos y Software de Base, en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

Objetivo

Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información.

Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

Definir los métodos de protección de la información crítica o sensible.

Alcance

Esta Política se aplica a todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes administrados por la SSEAF en donde residan los desarrollos mencionados.

Responsabilidad

La DGIC con la asistencia del Departamento de Seguridad de la Información, junto con el Propietario de la Información, definirán los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos.

La DGIC con la asistencia del Departamento de Seguridad de la Información, junto con el Propietario de la Información, definirán en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos.

Asimismo, el Departamento de Seguridad de la Información 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.

El Director de la DGIC asignará las funciones de "implementador" y "administrador de programas fuentes" al personal de su área que considere adecuado, cuyas responsabilidades se detallan en el presente capítulo. Asimismo, verificará el cumplimiento de las definiciones establecidas sobre los controles y las medidas de seguridad a ser incorporadas a los sistemas.

La DGIC incorporará aspectos relacionados con el licenciamiento, la calidad del software y la seguridad de la información en los contratos con terceros por el desarrollo de software.

Política

8.1. Requerimientos de Seguridad de los Sistemas

Objetivo

Garantizar que la seguridad sea una parte integral de los sistemas de información.

Los sistemas de información incluyen sistemas de operación, infraestructura, aplicaciones operativas, servicios y aplicaciones desarrolladas por el usuario. El diseño e implementación del sistema de información que soporta el proceso operativo puede ser crucial para la seguridad. Se deben identificar y acordar los requerimientos de seguridad antes del desarrollo y/o implementación de los sistemas de información.

8.1.1. Análisis y Especificaciones de los Requerimientos de Seguridad

Esta Política se implementa para incorporar seguridad a los sistemas de información (propios o de terceros) y a las mejoras o actualizaciones que se les incorporen.

Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema, como así también controles manuales de apoyo.

Se deben tener en cuenta las siguientes consideraciones:

a. Definir un procedimiento para que durante las etapas de análisis y diseño del sistema, se incorporen a los requerimientos, los correspondientes controles de seguridad. Este procedimiento debe incluir una etapa de evaluación de riesgos previa al diseño, para definir los requerimientos de seguridad e identificar los controles apropiados. En esta tarea deben participar las áreas usuarias, de sistemas, de seguridad informática y auditoría, especificando y aprobando los controles automáticos a incorporar al sistema y las necesidades de controles manuales complementarios. Las áreas involucradas podrán solicitar certificaciones y evaluaciones independientes para los productos a utilizar.

b. Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas.

c. Considerar que los controles introducidos en la etapa de diseño, son significativamente menos costosos de implementar y mantener que aquellos incluidos durante o después de la implementación.

8.2. Seguridad en los Sistemas de Aplicación

Objetivo

Para evitar la pérdida, modificación o uso inadecuado de los datos pertenecientes a los sistemas de información, se establecerán controles y registros de auditoría, verificando:

a. La validación de datos de entrada.

b. El procesamiento interno.

c. La autenticación de mensajes (interfaces entre sistemas).

d. La validación de datos de salida.

8.2.1. Validación de Datos de Entrada

Se definirá un procedimiento que durante la etapa de diseño, especifique controles que aseguren la validez de los datos ingresados, tan cerca del punto de origen como sea posible, controlando también datos permanentes y tablas de parámetros.

Este procedimiento considerará los siguientes controles:

a. Control de secuencia.

b. Control de monto límite por operación y tipo de usuario.

c. Control del rango de valores posibles y de su validez, de acuerdo a criterios predeterminados.

d. Control de paridad.

e. Control contra valores cargados en las tablas de datos.

f. Controles por oposición, de forma tal que quien ingrese un dato no pueda autorizarlo y viceversa.

Por otra parte, se llevarán a cabo las siguientes acciones:

a. Se definirá un procedimiento para realizar revisiones periódicas de contenidos de campos claves o archivos de datos, definiendo quién lo realizará, en qué forma, con qué método, quiénes deberán ser informados del resultado, etc.

b. Se definirá un procedimiento que explicite las alternativas a seguir para responder a errores de validación en un aplicativo.

c. Se definirá un procedimiento que permita determinar las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.

8.2.2. Controles de Procesamiento Interno

Se definirá un procedimiento para que durante la etapa de diseño, se incorporen controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores.

Para ello se implementarán:

a. Procedimientos que permitan identificar el uso y localización en los aplicativos, de funciones de incorporación y eliminación que realizan cambios en los datos.

b. Procedimientos que establezcan los controles y verificaciones necesarios para prevenir la ejecución de programas fuera de secuencia o cuando falle el procesamiento previo.

c. Procedimientos que establezcan la revisión periódica de los registros de auditoría de forma de detectar cualquier anomalía en la ejecución de las transacciones.

d. Procedimientos que realicen la validación de los datos generados por el sistema.

e. Procedimientos que verifiquen la integridad de los datos y del software cargado o descargado entre computadoras.

f. Procedimientos que controlen la integridad de registros y archivos.

g. Procedimientos que verifiquen la ejecución de los aplicativos en el momento adecuado.

h. Procedimientos que aseguren el orden correcto de ejecución de los aplicativos, la finalización programada en caso de falla, y la detención de las actividades de procesamiento hasta que el problema sea resuelto.

8.2.3. Autenticación de Mensajes

Cuando una aplicación tenga previsto el envío de mensajes que contengan información clasificada, se implementarán los controles criptográficos determinados en el punto “Controles Criptográficos”.

8.2.4. Validación de Datos de Salidas

Se establecerán procedimientos para validar la salida de los datos de las aplicaciones, incluyendo:

a. Comprobaciones de la razonabilidad para probar si los datos de salida son plausibles.

b. Control de conciliación de cuentas para asegurar el procesamiento de todos los datos.

c. Provisión de información suficiente, para que el lector o sistema de procesamiento subsiguiente determine la exactitud, totalidad, precisión y clasificación de la información.

d. Procedimientos para responder a las pruebas de validación de salidas.

e. Definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.

8.3. Controles Criptográficos

Objetivo

Se utilizarán sistemas y técnicas criptográficas para la protección de la información en base a un análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

Se debe establecer una gestión clave para sostener el uso de técnicas criptográficas.

8.3.1. Política de Utilización de Controles Criptográficos.

La SSEAF establece la presente Política de uso de controles criptográficos, a fin de determinar su correcto uso. Para ello se indica que:

a. Se utilizarán controles criptográficos en los siguientes casos:
   - Para la protección de claves de acceso a sistemas, datos y servicios.
   - Para la transmisión de información clasificada, fuera del ámbito de la SSEAF.
   - Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el Propietario de la Información y el Departamento de Seguridad de la Información

b. Se desarrollarán procedimientos respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al remplazo de las claves de cifrado.

c. El Director de la DGIC propondrá la asignación de funciones para:
   - Implementación de la Política de Controles Criptográficos.
   - Administración de Claves

d. Se deberá determinar con precisión el tipo de algoritmo de cifrado y la longitud de la clave, considerando aquellos que a la fecha se consideran seguros. Se recomienda verificar esta condición periódicamente con el objeto de efectuar las actualizaciones correspondientes.

8.3.2. Cifrado

Mediante la evaluación de riesgos que llevará a cabo el Propietario de la Información con la asistencia del Departamento de Seguridad de la Información, se identificará 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.

Al implementar la Política de la SSEAF en materia criptográfica, se considerarán los controles aplicables a la exportación e importación de tecnología criptográfica.

8.3.3. Firma Digital

Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos. Pueden aplicarse a cualquier tipo de documento que se procese electrónicamente. Se implementan mediante el uso de una técnica criptográfica sobre la base de

dos claves relacionadas de manera única, donde una clave, denominada privada, se utiliza para crear una firma y la otra, denominada pública, para verificarla.

Se tomarán recaudos para proteger la confidencialidad de las claves privadas.

Asimismo, es importante proteger la integridad de la clave pública. Esta protección se provee mediante el uso de un certificado de clave pública.

Se recomienda que las claves criptográficas utilizadas para firmar digitalmente no sean empleadas en procedimientos de cifrado de información. Dichas claves deben ser resguardadas bajo el control exclusivo de su titular.

Al utilizar firmas y certificados digitales, se considerará la legislación vigente y el conjunto de normas complementarias que fijan o modifican competencias y establecen procedimientos.

En algunos casos podría ser necesario establecer acuerdos especiales para respaldar el uso de las firmas digitales. A tal fin se deberá obtener asesoramiento legal con respecto al marco normativo aplicable y la modalidad del acuerdo a implementar.

8.3.4. Servicios de No Repudio

Estos servicios se utilizarán cuando sea necesario resolver disputas acerca de la ocurrencia de un evento o acción. Su objetivo es proporcionar herramientas para evitar que aquél que haya originado una transacción electrónica niegue haberla efectuado.

8.3.5. Protección de Claves Criptográficas

Se implementará un sistema de administración de claves criptográficas para respaldar la utilización por parte de la SSEAF de los dos tipos de técnicas criptográficas, a saber:

a. Técnicas de clave secreta (criptografía simétrica), cuando dos o más actores comparten la misma clave y ésta se utiliza tanto para cifrar información como para descifrarla.

b. Técnicas de clave pública (criptografía asimétrica), cuando cada usuario tiene un par de claves: una clave pública (que puede ser revelada a cualquier persona) utilizada para cifrar y una clave privada (que debe mantenerse en secreto) utilizada para descifrar. Las claves asimétricas utilizadas para cifrado no deben ser las mismas que se utilizan para firmar digitalmente.

Todas las claves serán protegidas contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada.

Se proporcionará una protección adecuada al equipamiento utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.

8.3.6. Protección de Claves Criptográficas: Normas y Procedimientos

Se redactarán las normas y procedimientos necesarios para:

a. Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.

b. Generar y obtener certificados de clave pública de manera segura.

c. Distribuir claves de forma segura a los usuarios que corresponda, incluyendo información sobre cómo deben activarse cuando se reciban.

d. Almacenar claves, incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados.

e. Cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las claves.

f. Revocar claves, incluyendo cómo deben retirarse o desactivarse las mismas, por ejemplo cuando las claves están comprometidas o cuando un usuario se desvincula de la SSEAF (en cuyo caso las claves también deben archivarse).

g. Recuperar claves perdidas o alteradas como parte de la administración de la continuidad de las actividades de la SSEAF, por ejemplo para la recuperación de la información cifrada.

h. Archivar claves, por ejemplo, para la información archivada o resguardada.

i. Destruir claves.

j. Registrar y auditar las actividades relativas a la administración de claves.

A fin de reducir la probabilidad de compromiso, se deberán definir fechas de inicio y caducidad de vigencia de las claves.

Además de la administración segura de las claves secretas y privadas, deberá tenerse en cuenta la protección de las claves públicas. Este problema es abordado mediante el uso de un certificado de clave pública. Este certificado se generará de forma que vincule de manera única la información relativa al propietario del par de claves pública/privada con la clave pública.

8.4. Seguridad de los Archivos del Sistema

Objetivo

Se garantizará que los desarrollos y actividades de soporte a los sistemas se lleven a cabo de manera segura, controlando el acceso a los archivos del mismo.

8.4.1. Software Operativo

Se definen los siguientes controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.

- Toda aplicación, desarrollada por la SSEAF o por un tercero tendrá un único responsable designado formalmente por el Director de la DGIC.
- Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.
- El Director de la DGIC, asignará la función de “implementador” al personal de su área que considere adecuado, quien tendrá como funciones principales:

  a. Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.

b. Asegurar que los sistemas aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.

c. Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del sector encargado del testeo y del usuario final.

d. Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida.

Otros controles a realizar son:

a. Guardar sólo los ejecutables en el ambiente de producción.

b. Llevar un registro de auditoría de las actualizaciones realizadas.

c. Retener las versiones previas del sistema, como medida de contingencia.

d. Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones y conformidades pertinentes, las pruebas previas a realizarse, etc.

e. Denegar permisos de modificación al implementador sobre los programas fuentes bajo su custodia.

f. Evitar, que la función de implementador sea ejercida por personal que pertenezca al sector de desarrollo o mantenimiento.

8.4.2. Protección de los Datos de Prueba del Sistema

Las pruebas de los sistemas se efectuarán sobre datos extraídos del ambiente operativo. Para proteger los datos de prueba se establecerán normas y procedimientos que contemplen lo siguiente:

a. Prohibir el uso de bases de datos operativas. En caso contrario se deben enmascarar los datos antes de su uso. Aplicar idénticos procedimientos de control de acceso que en la base de producción.

b. Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de tal autorización.

c. Eliminar inmediatamente, una vez completadas las pruebas, la información operativa utilizada.

8.4.3. Control de Cambios a Datos Operativos

La modificación, actualización o eliminación de los datos operativos serán realizadas a través de los sistemas que procesan dichos datos y de acuerdo al esquema de control de accesos implementado en los mismos. Una modificación por fuera de los sistemas a un dato, almacenado ya sea en un archivo o base de datos, podría poner en riesgo la integridad de la información.

Los casos en los que no fuera posible la aplicación de la precedente política, se considerarán como excepciones. El Departamento de Seguridad de la Información definirá procedimientos para la gestión de dichas excepciones que contemplarán lo siguiente:

a. Se generará una solicitud formal para la realización de la modificación, actualización o eliminación del dato.

b. El Propietario de la Información afectada, conjuntamente con el Director de la DGIC y el Departamento de Seguridad de la Información, aprobarán la ejecución del cambio evaluando las razones por las cuales se solicita.

c. Se generarán cuentas de usuario de emergencia para ser utilizadas en la ejecución de excepciones. Las mismas serán protegidas mediante contraseñas, sujetas al procedimiento de administración de contraseñas críticas y habilitadas sólo ante un requerimiento de emergencia y por el lapso que ésta dure.

d. Se designará un encargado de implementar los cambios, el cual no será personal del área de Desarrollo. En el caso de que esta función no pueda ser segregada, se aplicarán controles adicionales de acuerdo a lo establecido en los controles de separación de funciones.

e. Se registrarán todas las actividades realizadas con las cuentas de emergencia. Dicho registro será revisado posteriormente por el Departamento de Seguridad de la Información

8.4.4. Control de Acceso a las Bibliotecas de Programas Fuentes

Para reducir la probabilidad de alteración de programas fuentes, se aplicarán los siguientes controles:

a. El Responsable del Área Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda la función de “administrador de programas fuentes” al personal de su área que considere adecuado, quien tendrá en custodia los programas fuentes y deberá:

   - Proveer al Área de Desarrollo los programas fuentes solicitados para su modificación, manteniendo en todo momento la correlación programa fuente/ejecutable.
   - Llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, programador, Analista Responsable que autorizó, versión, fecha de última modificación y fecha/hora de compilación y estado (en modificación, en producción).
   - Verificar que el Analista Responsable que autoriza la solicitud de un programa fuente sea el designado para la aplicación, rechazando el pedido en caso contrario. Registrar cada solicitud aprobada.
   - Administrar las distintas versiones de una aplicación.
   - Asegurar que un mismo programa fuente no sea modificado simultáneamente por más de un desarrollador.

b. Denegar al “administrador de programas fuentes” permisos de modificación sobre los programas fuentes bajo su custodia.

c. Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen.

d. Establecer que el implementador de producción efectuará la generación del programa objeto o ejecutable que estará en producción (compilación), a fin de garantizar tal correspondencia.

e. Desarrollar un procedimiento que garantice que toda vez que se migre a producción el módulo fuente, se cree el código ejecutable correspondiente en forma automática.

f. Evitar que la función de "administrador de programas fuentes" sea ejercida por personal que pertenezca al sector de desarrollo y/o mantenimiento.

g. Prohibir la guarda de programas fuentes históricos (que no sean los correspondientes a los programas operativos) en el ambiente de producción.

h. Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuentes.

i. Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos por la SSEAF en los procedimientos que surgen de la presente política.

8.5. Seguridad de los Procesos de Desarrollo y Soporte

Objetivo

Esta Política provee seguridad al software y a la información del sistema de aplicación, por lo tanto se controlarán los entornos y el soporte dado a los mismos.

8.5.1. Procedimiento de Control de Cambios

A fin de minimizar los riesgos de alteración de los sistemas de información, se implementarán controles estrictos durante la implementación de cambios imponiendo el cumplimiento de procedimientos formales. Éstos garantizarán que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

Para ello se establecerá un procedimiento que incluya las siguientes consideraciones:

a. Verificar que los cambios sean propuestos por usuarios autorizados y respete los términos y condiciones que surjan de la licencia de uso.

b. Mantener un registro de los niveles de autorización acordados.

c. Solicitar la autorización del Propietario de la Información, en caso de tratarse de cambios a sistemas de procesamiento de la misma.

d. Efectuar un análisis de riesgos del cambio.

e. Determinar los requisitos de seguridad para el cambio.

f. Analizar el impacto de los cambios sobre los controles de seguridad existentes.

g. Obtener aprobación formal por parte del Director de la DGIC para las tareas detalladas, antes que comiencen las tareas.

h. Solicitar la revisión del Departamento de Seguridad de la Información para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.

i. Efectuar las actividades relativas al cambio en el ambiente de desarrollo.

j. Obtener la aprobación por parte del usuario autorizado y del área de pruebas mediante pruebas en el ambiente correspondiente.

k. Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.

l. Mantener un control de versiones para todas las actualizaciones de software.

m. Garantizar que la implementación se llevará a cabo minimizando la discontinuidad de las actividades y sin alterar los procesos involucrados.

n. Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operatoria.

o. Garantizar que sea el implementador quien efectúe el pasaje de los objetos modificados al ambiente operativo, de acuerdo a lo establecido en el control "Software Operativo".

8.5.2. Revisión Técnica de los Cambios en el Sistema Operativo

Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

Para ello, se definirá un procedimiento que incluya:

a. Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.

b. Garantizar que los cambios en el sistema operativo sean informados con anterioridad a la implementación.

c. Asegurar la actualización del Plan de Continuidad de las Actividades de la SSEAF.

8.5.3. Restricción del Cambio de Paquetes de Software

En caso de considerarlo necesario la modificación de paquetes de software suministrados por proveedores, y previa autorización del Responsable del Área Informática, se deberá:

a. Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.

b. Determinar la conveniencia de que la modificación sea efectuada por la SSEAF, por el proveedor o por un tercero.

c. Evaluar el impacto que se produce si la SSEAF se hace cargo del mantenimiento.

d. Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

8.5.4. Canales Ocultos y Código Malicioso

Un canal oculto (“*backdoor*”) puede exponer información utilizando algunos medios indirectos y desconocidos. El código malicioso está diseñado para afectar a un sistema en forma no autorizada y no requerida por el usuario.

En este sentido, se redactarán normas y procedimientos que incluyan:

a. Adquirir programas a proveedores acreditados o productos ya evaluados.

b. Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.

c. Controlar el acceso y las modificaciones al código instalado.

d. Utilizar herramientas para la protección contra la infección del software con código malicioso.

8.5.5. Desarrollo Externo de Software

Para el caso que se considere la tercerización del desarrollo de software, se establecerán normas y procedimientos que contemplen los siguientes puntos:

a. Acuerdos de licencias, propiedad de código y derechos conferidos (Ver Derechos de Propiedad Intelectual).

b. Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.

c. Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.

d. Verificación del cumplimiento de las condiciones de seguridad.

e. Acuerdos de custodia de los fuentes del software (y cualquier otra información requerida) en caso de quiebra de la tercera parte.

8.6. Gestión de vulnerabilidades técnicas

Objetivo

Se implementará la gestión de las vulnerabilidades técnicas de forma efectiva, sistemática y repetible, con mediciones que confirmen su efectividad. Dichas consideraciones incluirán los sistemas operativos, y cualquier otra aplicación en uso.

8.6.1. Vulnerabilidades técnicas

Se obtendrá información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, la exposición del Organismo a tales vulnerabilidades evaluadas, y se tomarán las medidas necesarias para tratar los riesgos asociados.

Para ello se contará con un inventario de software donde se detalle información de versiones del mismo así como datos del proveedor y responsable interno.

El proceso de gestión de las vulnerabilidades técnicas debe comprender:

a. Definición de roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas;

b. Procedimientos de identificación de vulnerabilidades técnicas potenciales;

c. Definición de una línea de tiempo para reaccionar ante las notificaciones de las vulnerabilidades técnicas potencialmente relevantes;

d. Definición de prioridades para la atención de necesidades relacionadas con actualizaciones de seguridad;

e. Identificación de los riesgos asociados y las acciones a llevar a cabo ante vulnerabilidades identificadas;

f. Identificación de los riesgos asociados a la instalación de parches;

g. Aprobación y evaluación de los parches antes de que sean instalados para garantizar que son efectivos y que no resultan en efectos secundarios que no puedan ser tolerados;

h. Consideración de controles alternativos en caso de inexistencia de parches;

i. Generación y mantenimiento de un registro de auditoría para todos los procedimientos emprendidos;

j. Seguimiento y evaluación regular del proceso de gestión de las vulnerabilidades técnicas para garantizar su efectividad y eficiencia.

9. Gestión de Incidentes de Seguridad

Generalidades

Existen numerosas amenazas que atentan contra la seguridad de la información, representando riesgos latentes que de materializarse pueden ocasionar incidentes de seguridad.

LA SSEAF cuenta con innumerables activos de información, cada uno de los cuales puede encontrarse expuesto a sufrir incidentes de seguridad. Es por ello que resulta sumamente necesario contar con una capacidad de gestión de dichos incidentes que permita comenzar por su detección, llevar a cabo su tratamiento y colaborar en la prevención de futuros incidentes similares.

Objetivo

Garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.

Alcance

La Política definida en este documento se aplica a todo incidente que pueda afectar la seguridad de la información de la SSEAF.

Responsabilidad

La DGIC será responsable de implementar los medios y canales necesarios para que el Departamento de Seguridad de la Información maneje 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 Departamento de Seguridad de la Información tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados así como su comunicación a la DGIC, a los propietarios de la información y a los organismos nacionales de Ciberseguridad.

Todo el personal de la SSEAF es responsable de reportar debilidades e incidentes de seguridad que oportunamente se detecten.

Política

9.1. Informe de los eventos y debilidades de la seguridad de la información

Objetivo

Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna.

9.1.1. Reporte de los eventos de la seguridad de información

Los incidentes relativos a la seguridad serán comunicados a través de las autoridades o canales 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 Departamento de Seguridad de la Información 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 a la DGIC al tanto de la ocurrencia de incidentes de seguridad.

Todos los empleados y contratistas deben conocer fehacientemente el procedimiento de comunicación de incidentes de seguridad, y deben informar formalmente los mismos tan pronto hayan tomado conocimiento de su ocurrencia.

9.1.2. Reporte de las debilidades de la seguridad

Los usuarios de servicios de información, al momento de tomar conocimiento directa o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar formalmente las mismas al Responsable de Seguridad de la Información.

Se prohíbe expresamente a los usuarios la realización de pruebas para detectar y/o utilizar una supuesta debilidad o falla de seguridad.

9.1.3. Comunicación de Anomalías del Software

Se establecerán procedimientos para la comunicación de anomalías de software, los cuales deben contemplar:

a. Registrar los síntomas del problema y los mensajes que aparecen en pantalla.

b. Establecer las medidas de aplicación inmediata ante la presencia de una anomalía.

c. Alertar inmediatamente de modo formal al Departamento de Seguridad de la Información o al responsable del Activo de que se trate.

Se prohíbe a los usuarios eliminar el software que supuestamente tiene una anomalía, a menos que estén autorizados formalmente para hacerlo. La recuperación será realizada por personal experimentado, adecuadamente habilitado.

9.2. Gestión de los Incidentes y mejoras de la seguridad de la información

Objetivo

Asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información.

Se deben establecer las responsabilidades y procedimientos para manejar de manera efectiva los eventos y debilidades en la seguridad de la información una vez que han sido reportados. Se debe aplicar un proceso de mejora continua para la respuesta, monitoreo, evaluación y gestión general de los incidentes en la seguridad de la información.

9.2.1. Responsabilidades y procedimientos

Se establecerán funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad. 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.
    3. Negociación de compensaciones por parte de los proveedores de software y de servicios.

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 Dirección y revisión de su cumplimiento.

4. Constatación de la integridad de los controles y sistemas de la SSEAF en un plazo mínimo.

En los casos en los que se considere necesario, se solicitará la participación del Responsable del Área Jurídica de la SSEAF en el tratamiento de incidentes de seguridad ocurridos.

9.2.2. Aprendiendo a partir de los incidentes de la seguridad de la información

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.

9.2.3. Procesos Disciplinarios

Se seguirá el proceso disciplinario formal contemplado en las normas que rigen al personal de la Administración Pública, para los empleados que violen la Política, Normas y Procedimientos de Seguridad del Organismo

10. Gestión de la Continuidad

Generalidades

La administración de la continuidad de las actividades es un proceso crítico que debe involucrar a todos los niveles de la SSEAF.

El desarrollo e implementación de planes de contingencia es una herramienta básica para garantizar que las actividades de la SSEAF puedan restablecerse dentro de los plazos requeridos.

Dichos planes deben mantenerse actualizados y transformarse en una parte integral del resto de los procesos de administración y gestión, debiendo incluir necesariamente controles destinados a identificar y reducir riesgos, atenuar las consecuencias de eventuales interrupciones de las actividades de la SSEAF y asegurar la reanudación oportuna de las operaciones indispensables.

Objetivo

Minimizar los efectos de las posibles interrupciones de las actividades normales de la SSEAF (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.

Maximizar la efectividad de las operaciones de contingencia de la SSEAF con el establecimiento de planes que incluyan al menos las siguientes etapas:

a. *Notificación / Activación*: Consistente en la detección y determinación del daño y la activación del plan.

b. *Reanudación*: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.

c. *Recuperación*: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

Asegurar la coordinación con el personal de la SSEAF y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

Alcance

Esta Política se aplica a todos los procesos críticos identificados de la SSEAF.

Responsabilidad

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

Los Propietarios de la Información y el Departamento de Seguridad de la Información cumplirán las siguientes funciones:

- Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades de la SSEAF.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones.
- Identificar los controles preventivos.
- Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades de la SSEAF.
- Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades de la SSEAF.

Los Responsables de Procesos revisarán periódicamente los planes bajo su incumbencia, como así también identificar cambios en las disposiciones relativas a las actividades de la SSEAF 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.

La DGIC tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información de la SSEAF frente a interrupciones imprevistas.

Política

10.1. Categoría: Gestión de continuidad del Organismo

Objetivo

Contraatacar las interrupciones a las actividades del organismo y proteger los procesos críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

10.1.1. Proceso de Administración de la Continuidad de la SSEAF

La DGIC será el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de las actividades de la SSEAF.

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

a. Identificar y priorizar los procesos críticos de las actividades de la SSEAF.
b. Asegurar que todos los integrantes de la SSEAF 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 de la SSEAF.
c. Elaborar y documentar una estrategia de continuidad de las actividades de la SSEAF consecuente con los objetivos y prioridades acordados.
d. Proponer planes de continuidad de las actividades de la SSEAF 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.

g. Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades de la SSEAF.

h. Proponer las modificaciones a los planes de contingencia.

10.1.2. Continuidad de las Actividades y Análisis de los Impactos

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

- 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 e incendio, desastres naturales, destrucción edilicia, atentados, etc.
- 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.
- 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 backup, los registros no electrónicos vitales, etc.

Esta actividad será llevada a cabo con la activa participación de los propietarios de los procesos y recursos de información de que se trate y el Departamento de Seguridad de la Información, conjuntamente con el Director de la DGIC, considerando todos los procesos de las actividades de la SSEAF 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 de la SSEAF. Una vez que se ha creado este plan, el mismo debe ser propuesto a la máxima autoridad de la SSEAF para su aprobación.

10.1.3. Elaboración e Implementación de los Planes de Continuidad de la SSEAF

Los propietarios de procesos y recursos de información, con la asistencia del Departamento de Seguridad de la Información, elaborarán los planes de contingencia necesarios para garantizar la continuidad de las actividades de la SSEAF. Estos procesos deberán ser propuestos por la DGIC.

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.

Asimismo, el proceso de planificación debe concentrarse en los objetivos de las actividades de la SSEAF requeridos, 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.

10.1.4. Marco para la Planificación de la Continuidad de las Actividades de la SSEAF

Se mantendrá un solo marco para los planes de continuidad de las actividades de la SSEAF, 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.

Estas modificaciones deberán ser propuestas por la DGIC para su aprobación.

El marco para la planificación de la continuidad de las actividades de la SSEAF, 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 de la SSEAF 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 de la SSEAF 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 de la SSEAF.

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 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.

La SSEAF deberá definir formalmente los administradores de los planes de contingencia.

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.

10.1.5. Ensayo, Mantenimiento y Reevaluación de los Planes de Continuidad de la SSEAF.

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

- La DGIC establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.
- El cronograma indicará quienes son los responsables de llevar a cabo cada una de las pruebas y de elevar el resultado obtenido a la DGIC.

Se deberán 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).

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 la SSEAF, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones.

Para las operaciones críticas de la SSEAF se tomarán en cuenta, además, los siguientes mecanismos:

a. Efectuar pruebas de recuperación en un sitio alternativo (ejecutando los procesos de las actividades de la SSEAF 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).

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

La periodicidad de revisión de los planes de contingencia será formalmente definida por la SSEAF.

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 de la SSEAF aún no reflejadas en dichos planes.

Deberá prestarse atención, especialmente, a los cambios de:

a. Personal.

b. Direcciones o números telefónicos.

c. Estrategia de la SSEAF.

d. Ubicación, instalaciones y recursos.

e. Legislación.

f. Contratistas, proveedores y clientes críticos.

g. Procesos, o procesos nuevos / eliminados.

h. Tecnologías.

i. Requisitos operacionales.

j. Requisitos de seguridad.

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 la DGIC para su aprobación por el superior jerárquico que corresponda.

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.

11. Cumplimiento

Generalidades

El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales.

Los requisitos normativos y contractuales pertinentes a cada sistema de información deben estar debidamente definidos y documentados.

El Área Legal de la SSEAF, será responsable de encuadrar jurídicamente la formulación e implementación de la política.

Objetivos

Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas al Organismo y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.

Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad de la SSEAF.

Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

Optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.

Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías de sistemas.

Determinar los plazos para el mantenimiento de información y para la recolección de evidencia de la SSEAF.

Alcance

Esta Política se aplica a todo el personal de la SSEAF, cualquiera sea su situación de revista.

Asimismo se aplica a los sistemas de información, normas, procedimientos, documentación y plataformas técnicas de la SSEAF y a las auditorías efectuadas sobre los mismos.

Responsabilidad

El Departamento de Seguridad de la Información cumplirá las siguientes funciones:

- 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 todas las áreas de la SSEAF a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad.
- Verificar periódicamente que los sistemas de información cumplan la política, normas y procedimientos de seguridad establecidos.

- Garantizar la seguridad y el control de las herramientas utilizadas para las revisiones de auditoría.

El Responsable del Área Legal de la SSEAF, con la asistencia del Departamento de Seguridad de la Información cumplirá las siguientes funciones:

- Definir y documentar claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información.
- Redactar un Compromiso de Confidencialidad a ser firmado por todo el personal.

Los Directores de la SSEAF velarán por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos en la presente Política, dentro de su área de responsabilidad.

Todos los empleados de los mandos medios y superiores conocerán, comprenderán, darán a conocer, cumplirán y harán cumplir la presente Política y la normativa vigente.

Política

11.1. Cumplimiento de Requisitos Legales

Objetivo

Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad.

El diseño, operación, uso y gestión de los sistemas de información pueden estar sujetos a requerimientos de seguridad estatutarios, reguladores y contractuales.

11.1.1. Identificación de la Legislación Aplicable

Se definirán y documentarán claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información. Del mismo modo se definirán y documentarán los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos.

11.1.2. Derechos de Propiedad Intelectual

Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

Los empleados únicamente podrán utilizar material autorizado por la SSEAF.

La SSEAF solo podrá autorizar el uso de material producido por el mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

La infracción a estos derechos puede tener como resultado acciones legales que podrían derivar en demandas penales.

El software es considerado una obra intelectual que goza de la protección de las leyes.

Los productos de software se suministran normalmente bajo acuerdos de licencia que suelen limitar el uso de los productos al equipamiento específico y su copia a la creación de copias de resguardo solamente.

La DGIC con la asistencia del Departamento de Seguridad de la Información, analizará los términos y condiciones de la licencia, e implementará los siguientes controles:

a. Definir normas y procedimientos para el cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software.

b. Divulgar las políticas de adquisición de software y las disposiciones de la Ley de Propiedad Intelectual, y notificar la determinación de tomar acciones disciplinarias contra el personal que las infrinja.

c. Mantener un adecuado registro de activos.

d. Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.

e. Implementar controles para evitar el exceso del número máximo permitido de usuarios.

f. Verificar que sólo se instalen productos con licencia y software autorizado.

g. Elaborar y divulgar un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.

h. Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros.

i. Utilizar herramientas de auditoría adecuadas.

j. Cumplir con los términos y condiciones establecidos para obtener software e información en redes públicas.

11.1.3. Protección de los Registros de la SSEAF

Los registros críticos de la SSEAF se protegerán contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales de la SSEAF.

Los registros se clasificarán en diferentes tipos, por ejemplo registros contables, registros de base de datos, registros de auditoría y procedimientos operativos, cada uno de ellos detallando los períodos de retención y el tipo de medios de almacenamiento, por ejemplo papel, microfichas, medios magnéticos u ópticos.

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 (Ver 10.3. Controles Criptográficos).

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.(Ver 10.3.1. Política de Utilización de Controles Criptográficos.)

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.

Los sistemas de almacenamiento de datos serán seleccionados de modo tal que los datos requeridos puedan recuperarse de una manera que resulte aceptable para un tribunal de justicia, por ejemplo que todos los registros requeridos puedan recuperarse en un plazo y un formato aceptable.

El sistema de almacenamiento y manipulación garantizará una clara identificación de los registros y de su período de retención legal o normativa. Asimismo, se permitirá una adecuada destrucción de los registros una vez transcurrido dicho período, si ya no resultan necesarios para la SSEAF.

A fin de cumplir con estas obligaciones, se tomarán las siguientes medidas:

a. Elaborar y divulgar los lineamientos para la retención, almacenamiento, manipulación y eliminación de registros e información.

b. Preparar un cronograma de retención identificando los tipos esenciales de registros y el período durante el cual deben ser retenidos.

c. Mantener un inventario de programas fuentes de información clave.

d. Implementar adecuados controles para proteger la información y los registros esenciales contra pérdida, destrucción y falsificación.

11.1.4. Protección de Datos y Privacidad de la Información Personal

Todos los empleados deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones.

La SSEAF redactará un “Compromiso de Confidencialidad”, el cual deberá ser suscrito por todos los empleados. La copia firmada del compromiso será retenida en forma segura por la SSEAF.

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 deberá 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 (Ver 6. Seguridad del Personal).

11.1.5. Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información

Los recursos de procesamiento de información de la SSEAF se suministran con un propósito determinado. Toda utilización de estos recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos debe ser considerada como uso indebido.

Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo.

11.1.6. Recolección de Evidencia

Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria estará descrita en los procedimientos internos.

Cuando la acción implique la aplicación de una ley, tanto civil como penal, la evidencia presentada debe cumplir con lo establecido por las normas procesales. Para lograr la validez de la evidencia, la SSEAF garantizará que sus sistemas de información cumplen con la normativa y los estándares o códigos de práctica relativos a la producción de evidencia válida.

Para lograr la calidad y totalidad de la evidencia es necesaria una sólida pista de la misma. Esta pista se establecerá cumpliendo las siguientes condiciones:

a. Almacenar los documentos en papel originales en forma segura y mantener registros acerca de quién lo halló, dónde se halló, cuándo se halló y quién presenció el hallazgo. Cualquier investigación debe garantizar que los originales no sean alterados.

b. Copiar la información para garantizar su disponibilidad. Se mantendrá un registro de todas las acciones realizadas durante el proceso de copia. Se almacenará en forma segura una copia de los medios y del registro.

Cuando se detecta un incidente, puede no resultar obvio si éste derivará en una demanda legal por lo tanto se deben tomar todos los recaudos establecidos para la obtención y preservación de la evidencia.

11.2. Revisiones de la Política de Seguridad y la Compatibilidad Técnica

Objetivo

Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.

La seguridad de los sistemas de información se debiera revisar regularmente.

Estas revisiones deben realizarse en base a las políticas de seguridad apropiadas y las plataformas técnicas, y los sistemas de información deben ser auditados en cumplimiento con los estándares de implementación de seguridad aplicables y los controles de seguridad documentados.

11.2.1. Cumplimiento de la Política de Seguridad

Cada Responsable de Unidad Organizativa, velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad.

El Departamento de Seguridad de la Información, realizará revisiones periódicas de todas las áreas de la SSEAF a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. Entre las áreas a revisar se incluyen las siguientes:

a. Sistemas de información.

b. Proveedores de sistemas.

c. Propietarios de información.

d. Usuarios.

Los Propietarios de la Información brindarán apoyo a la revisión periódica del cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables.

11.2.2. Verificación de la Compatibilidad Técnica

El Departamento de Seguridad de la Información verificará periódicamente que los sistemas de información cumplan con la política, normas y procedimientos de seguridad, las que incluirán la revisión de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados. En caso de ser necesario, estas revisiones contemplarán la asistencia técnica especializada.

El resultado de la evaluación se volcará en un informe técnico para su ulterior interpretación por parte de los especialistas. Para ello, la tarea podrá ser realizada por un profesional experimentado (en forma manual o con el apoyo de herramientas de software), o por un paquete de software automatizado que genere reportes que serán interpretados por un especialista técnico.

La verificación del cumplimiento comprenderá pruebas de penetración y tendrá como objetivo la detección de vulnerabilidades en el sistema y la verificación de la eficacia de los controles con relación a la prevención de accesos no autorizados. Se tomarán los recaudos necesarios en el caso de pruebas de penetración exitosas que comprometan la seguridad del sistema.

Las verificaciones de cumplimiento sólo serán realizadas por personas competentes, formalmente autorizadas y bajo la supervisión.

11.3. Sanciones Previstas por Incumplimiento

Se sancionará administrativamente a todo aquel que viole lo dispuesto en la presente Política de Seguridad conforme a lo dispuesto por las normas que rigen al personal de la Administración Pública, y en caso de corresponder, se realizarán las acciones correspondientes ante el o los Organismos pertinentes. Las sanciones sólo pueden imponerse mediante un acto administrativo que así lo disponga cumpliendo las formalidades impuestas por los preceptos constitucionales y las demás normativas específicas aplicables. Adicionalmente a las sanciones disciplinarias o administrativas, el funcionario que no da debido cumplimiento a sus obligaciones pueden incurrir también en responsabilidad civil o patrimonial cuando ocasiona un daño que debe ser indemnizado- y/o en responsabilidad penal -cuando su conducta constituye un comportamiento considerado delito por el Código Penal y leyes especiales.