



# **UNIVERSIDAD TÉCNICA DEL NORTE**

**FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS**

**CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES**

**TEMA:**

**ELABORACIÓN E IMPLEMENTACIÓN DEL MANUAL DE POLÍTICAS  
Y NORMAS DE SEGURIDAD INFORMÁTICA PARA LA EMPRESA  
ELÉCTRICA REGIONAL NORTE S.A. – EMELNORTE.**

**AUTOR:** EGDA. ANA CRISTINA OREJUELA PÉREZ

**DIRECTOR:** ING. EDGAR DANIEL JARAMILLO

**IBARRA – ECUADOR**

**2014**



# UNIVERSIDAD TÉCNICA DEL NORTE

## BIBLIOTECA UNIVERSITARIA

### AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

#### 1. IDENTIFICACIÓN DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD	100256476 – 1		
APELLIDOS Y NOMBRES	ANA CRISTINA OREJUELA PÉREZ		
DIRECCIÓN	CARLOS EMILIO GRIJALVA Y ROCAFUERTE		
EMAIL	<a href="mailto:kristy_op@hotmail.com">kristy_op@hotmail.com</a>		
TELÉFONO FIJO	062600367	TELÉFONO MÓVIL	0999027678

DATOS DE LA OBRA	
TÍTULO	ELABORACIÓN E IMPLEMENTACIÓN DEL MANUAL DE POLÍTICAS Y NORMAS DE SEGURIDAD INFORMÁTICA PARA LA EMPRESA ELÉCTRICA REGIONAL NORTE S.A. – EMELNORTE.
AUTOR	ANA CRISTINA OREJUELA PÉREZ
FECHA	20 DE NOVIEMBRE DE 2014
PROGRAMA	PREGADO
TÍTULO POR EL QUE OPTA	INGENIERÍA EN SISTEMAS COMPUTACIONALES
DIRECTOR	ING. EDGAR DANIEL JARAMILLO



## UNIVERSIDAD TÉCNICA DEL NORTE

### AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

#### 2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Ana Cristina Orejuela Pérez, con cedula de ciudadanía Nro. 100256476 – 1, en calidad de autor y titular de los derechos patrimoniales del trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en formato digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión en concordancia con la Ley de Educación Superior Artículo 144.

Firma

Nombre: ANA CRISTINA OREJUELA PÉREZ

Cédula: 100256476 – 1

Ibarra a los veinte días del mes de Noviembre del 2014



# UNIVERSIDAD TÉCNICA DEL NORTE

## CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE INVESTIGACIÓN

### A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, Ana Cristina Orejuela Pérez, con cedula de ciudadanía Nro. 100256476 – 1, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, articulo 4, 5 y 6, en calidad de autor del trabajo de grado denominado: **“ELABORACIÓN E IMPLEMENTACIÓN DEL MANUAL DE POLÍTICAS Y NORMAS DE SEGURIDAD INFORMÁTICA PARA LA EMPRESA ELÉCTRICA REGIONAL NORTE S.A. – EMELNORTE”** que ha sido desarrollado para optar por el título de Ingeniería en Sistemas Computacionales en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte

Firma

Nombre: ANA CRISTINA OREJUELA PÉREZ

Cédula: 100256476 – 1

Ibarra a los veinte días del mes de Noviembre del 2014



## UNIVERSIDAD TÉCNICA DEL NORTE

### CERTIFICACIÓN

Certifico que la tesis “ELABORACIÓN E IMPLEMENTACIÓN DEL MANUAL DE POLÍTICAS Y NORMAS DE SEGURIDAD INFORMÁTICA PARA LA EMPRESA ELÉCTRICA REGIONAL NORTE S.A. – EMELNORTE” ha sido realizada en su totalidad por la señorita Ana Cristina Orejuela Pérez, portadora de la cédula de ciudadanía número: 100256476 – 1.



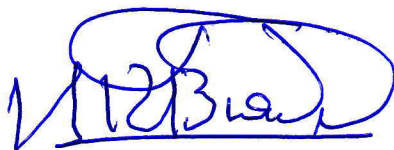
Ing. Edgar Daniel Jaramillo  
DIRECTOR DE LA TESIS

## CERTIFICACIÓN

Siendo auspiciante del proyecto de tesis de la Egresada Ana Cristina Orejuela Pérez con C.I.: 1002564761, quien desarrolló su trabajo con el tema **“ELABORACIÓN E IMPLEMENTACIÓN DEL MANUAL DE POLÍTICAS Y NORMAS DE SEGURIDAD INFORMÁTICA PARA LA EMPRESA ELÉCTRICA REGIONAL NORTE S.A. – EMELNORTE”**, me es grato informar que se han superado con satisfacción la implementación del manual de políticas y normas de seguridad informática, por lo que se recibe el proyecto como culminado y realizado por parte de la egresada Ana Cristina Orejuela Pérez. Una vez que hemos recibido la documentación y producto resultante, nos comprometemos a continuar utilizando los recursos entregados a la Institución.

La egresada Ana Cristina Orejuela Pérez puede hacer uso de este documento para los fines pertinentes en la Universidad Técnica del Norte.

Atentamente,



Ing. René Brown

**DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN  
EMPRESA ELÉCTRICA REGIONAL NORTE S.A. – EMELNORTE**



# UNIVERSIDAD TÉCNICA DEL NORTE

## DEDICATORIA

*A mi padre querido, Miguel Antonio Orejuela Bolaños, que fue, es y será mi guía y mi protector, supo darme fuerzas y su apoyo incondicional para seguir adelante y cumplir todas mis metas. Estará presente todos los días de mi vida.*

*A mi madre, Nancy Elizabeth Pérez Quinteros, quien me ha apoyado para llegar a culminar esta etapa de mis estudios, ya que siempre me ha brindado el mejor ejemplo y ha estado presente en todo momento.*

*A mi hermano, Miguel Eduardo, por sus ánimos y buenos deseos de siempre seguir adelante.*



# UNIVERSIDAD TÉCNICA DEL NORTE

## AGRADECIMIENTO

*A Dios, por haberme guiado por un buen camino y lograr con éxito esta etapa de mi vida estudiantil.*

*A todos los miembros de mi familia, por sus ánimos y su apoyo incondicional.*

*A la Universidad Técnica del Norte, por abrirme sus puertas y prepararme adecuadamente en sus aulas y con los mejores docentes que me impartieron sus conocimientos.*

*A mi director de tesis, Ing. Edgar Daniel Jaramillo, por sus recomendaciones, consejos y su amistad.*

*A todos los docentes de la UTN, por su paciencia durante toda mi etapa estudiantil.*

*A todos los amigos que han estado presentes en las buenas y en las malas.*





# UNIVERSIDAD TÉCNICA DEL NORTE

## RESUMEN

El presente documento tiene como finalidad dar a conocer las políticas y normas de Seguridad Informática que deberán observar los usuarios de servicios de tecnologías de información, para proteger adecuadamente los activos tecnológicos y la información de la EMPRESA ELÉCTRICA REGIONAL NORTE S.A. – EMELNORTE.

En términos generales estas políticas de seguridad informática, propende por englobar los procedimientos más adecuados, tomando como lineamientos principales cuatro criterios, que se detallan a continuación:

**Seguridad Organizacional:** Dentro de este, se establece el marco formal de seguridad que debe sustentar la EMPRESA ELÉCTRICA REGIONAL NORTE S.A. – EMELNORTE, incluyendo servicios o contrataciones externas a la infraestructura de seguridad, integrando el recurso humano con la tecnología, denotando responsabilidades y actividades complementarias como respuesta ante situaciones anómalas a la seguridad.

**Seguridad Lógica:** Trata de establecer e integrar los mecanismos y procedimientos, que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades, perfiles de seguridad, control de acceso a las aplicaciones y documentación sobre sistemas, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, selección y aceptación de sistemas, hasta el control de software malicioso.

**Seguridad Física:** Identifica los límites mínimos que se deben cumplir en cuanto a perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en la importancia de los activos.

**Seguridad Legal:** Integra los requerimientos de seguridad que deben cumplir todos los funcionarios, asociados y usuarios de la red institucional bajo la reglamentación de la normativa interna de la EMPRESA ELÉCTRICA REGIONAL NORTE S.A. – EMELNORTE; en cuanto al recurso humano, tendrá sanciones aplicables ante faltas cometidas de acuerdo con la Ley o la normativa interna estipulada.



# UNIVERSIDAD TÉCNICA DEL NORTE

## SUMMARY

The present document aims to present the policies and information security standards to be observed by users of information technology services to properly protect information technology assets and the EMPRESA ELÉCTRICA REGIONAL NORTE S.A. – EMELNORTE.

In general, these computer security policies, tends to encompass the most appropriate procedures, on the main outlines four criteria, which are detailed below:

**Organizational Security:** Within this, the formal security framework which should underpin the EMPRESA ELÉCTRICA REGIONAL NORTE S.A. – EMELNORTE, including services or external security infrastructure procurement, human resource integrating technology, denoting responsibilities and activities such as abnormal response to security situations.

**Logical Security:** Try to establish and integrate the mechanisms and procedures that allow monitor access to information assets, which include user management procedures, defined responsibilities, security profiles, access control applications and documentation systems, ranging from the control of changes in equipment configuration, incident management, selection and acceptance of systems to control the malicious software.

**Physical Security:** Identifies the minimum limits that must be met in terms of security perimeters, so that they can establish controls in handling equipment, transfer of information and control access to different areas based on the importance of active.

**Legal Security:** Integrates security requirements to be met by all staff members and users of the corporate network in the regulation of the internal regulations of the EMPRESA ELÉCTRICA REGIONAL NORTE S.A. – EMELNORTE; in terms of human resources, will face misconduct penalties according to the law or internal policy as stated.

# TABLA DE CONTENIDOS

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE .....	ii
CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE INVESTIGACIÓN .....	iv
CERTIFICACIÓN .....	v
DEDICATORIA .....	vii
AGRADECIMIENTO .....	viii
RESUMEN.....	ix
SUMMARY .....	x
TABLA DE CONTENIDOS.....	xi
ÍNDICE DE GRÁFICOS .....	xx
CAPÍTULO I.....	1
1 INTRODUCCIÓN .....	1
1.1 ANTECEDENTES.....	1
1.1.1 MISIÓN.....	1
1.1.2 VISIÓN .....	1
1.1.3 ORGANIZACIÓN DE LA EMPRESA.....	2
1.2 PROBLEMA.....	2
1.3 OBJETIVOS.....	3
1.3.1 OBJETIVO GENERAL .....	3
1.3.2 OBJETIVOS ESPECÍFICOS.....	3
1.4 JUSTIFICACIÓN.....	4
1.5 ALCANCE.....	4
CAPÍTULO II.....	7
2 MARCO TEÓRICO .....	7
2.1 DEFINICIÓN DE LA SEGURIDAD INFORMÁTICA.....	7
2.1.1 SEGURIDAD INFORMÁTICA .....	7
2.1.2 AMENAZAS .....	8

2.1.3 ANÁLISIS DE RIESGOS .....	9
2.1.4 POLÍTICAS DE SEGURIDAD .....	10
2.1.5 RESPALDO .....	11
2.2 NORMA TÉCNICA ECUATORIANA INEN-ISO/IEC 27002:2009 .....	12
2.2.1 EVALUACIÓN Y TRATAMIENTO DE RIESGOS .....	12
2.2.1.1 EVALUACIÓN DE LOS RIESGOS DE SEGURIDAD .....	12
2.2.1.2 TRATAMIENTO DE LOS RIESGOS DE LA SEGURIDAD .....	13
2.2.2 POLÍTICA DE LA SEGURIDAD .....	15
2.2.2.1 DOCUMENTO DE LA POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN .	15
2.2.2.2 REVISIÓN DE LA POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN .....	16
2.2.3 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.....	18
2.2.3.1 ORGANIZACIÓN INTERNA.....	18
2.2.3.1.1 COMPROMISO DE LA DIRECCIÓN CON LA SEGURIDAD DE LA INFORMACIÓN .....	19
2.2.3.1.2 COORDINACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN .....	20
2.2.3.1.3 ASIGNACIÓN DE RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN .....	21
2.2.3.1.4 PROCESO DE AUTORIZACIÓN PARA LOS SERVICIOS DE PROCESAMIENTO DE LA INFORMACIÓN .....	23
2.2.3.1.5 ACUERDOS SOBRE CONFIDENCIALIDAD .....	23
2.2.3.1.6 CONTACTO CON LAS AUTORIDADES.....	25
2.2.3.1.7 CONTACTOS CON GRUPOS DE INTERÉS ESPECIALES .....	26
2.2.3.1.8 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN....	27
2.2.3.2 PARTES EXTERNAS.....	28
2.2.3.2.1 IDENTIFICACIÓN DE LOS RIESGOS RELACIONADOS CON LAS PARTES EXTERNAS .....	29
2.2.4 GESTIÓN DE ACTIVOS .....	35
2.2.4.1 RESPONSABILIDAD POR LOS ACTIVOS .....	35
2.2.4.1.1 INVENTARIO DE ACTIVOS .....	35
2.2.4.1.2 RESPONSABLE DE LOS ACTIVOS.....	37

2.2.4.1.3	USO ACEPTABLE DE LOS ACTIVOS.....	38
2.2.4.2	CLASIFICACIÓN DE LA INFORMACIÓN .....	39
2.2.4.2.1	DIRECTRICES DE CLASIFICACIÓN.....	39
2.2.4.2.2	ETIQUETADO Y MANEJO DE LA INFORMACIÓN .....	40
2.2.5	GESTIÓN DE COMUNICACIONES Y OPERACIONES.....	41
2.2.5.1	PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES.....	41
2.2.5.1.1	DOCUMENTACIÓN DE LOS PROCEDIMIENTOS DE OPERACIÓN.....	42
2.2.5.1.2	GESTIÓN DEL CAMBIO.....	43
2.2.5.1.3	DISTRIBUCIÓN DE FUNCIONES .....	44
2.2.5.1.4	SEPARACIÓN DE LAS INSTALACIONES DE DESARROLLO, ENSAYO Y OPERACIÓN .....	45
2.2.5.2	GESTIÓN DE LA PRESTACIÓN DEL SERVICIO POR TERCERAS PARTES ..	47
2.2.5.2.1	PRESTACIÓN DEL SERVICIO.....	47
2.2.5.2.2	MONITOREO Y REVISIÓN DE LOS SERVICIOS POR TERCEROS .....	48
2.2.5.2.3	GESTIÓN DE LOS CAMBIOS EN LOS SERVICIOS POR TERCERAS PARTES .....	49
2.2.5.3	PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA.....	50
2.2.5.3.1	GESTIÓN DE LA CAPACIDAD.....	51
2.2.5.3.2	ACEPTACIÓN DEL SISTEMA .....	52
2.2.5.4	PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS Y MÓVILES.....	53
2.2.5.4.1	CONTROLES CONTRA CÓDIGOS MALICIOSOS.....	54
2.2.5.4.2	CONTROLES CONTRA CÓDIGOS MÓVILES .....	56
2.2.5.5	RESPALDO .....	57
2.2.5.5.1	RESPALDO DE LA INFORMACIÓN.....	57
2.2.5.6	GESTIÓN DE LA SEGURIDAD DE LAS REDES .....	59
2.2.5.6.1	CONTROLES DE LAS REDES.....	59
2.2.5.6.2	SEGURIDAD DE LOS SERVICIOS DE LA RED.....	60
2.2.5.7	MANEJO DE LOS MEDIOS .....	61
2.2.5.7.1	GESTIÓN DE LOS MEDIOS REMOVIBLES.....	62
2.2.5.7.2	ELIMINACIÓN DE LOS MEDIOS.....	63

2.2.5.7.3	PROCEDIMIENTOS PARA EL MANEJO DE LA INFORMACIÓN .....	64
2.2.5.7.4	SEGURIDAD DE LA DOCUMENTACIÓN DEL SISTEMA .....	65
2.2.5.8	INTERCAMBIO DE LA INFORMACIÓN.....	66
2.2.5.8.1	POLÍTICAS Y PROCEDIMIENTOS PARA EL INTERCAMBIO DE INFORMACIÓN .....	66
2.2.5.8.2	ACUERDOS PARA EL INTERCAMBIO.....	69
2.2.5.8.3	MEDIOS FÍSICOS EN TRÁNSITO.....	71
2.2.5.8.4	MENSAJERÍA ELECTRÓNICA.....	72
2.2.5.8.5	SISTEMAS DE INFORMACIÓN DEL NEGOCIO .....	73
2.2.5.9	SERVICIOS DE COMERCIO ELECTRÓNICO.....	75
2.2.5.9.1	COMERCIO ELECTRÓNICO .....	75
2.2.5.9.2	TRANSACCIONES EN LÍNEA.....	77
2.2.5.9.3	INFORMACIÓN DISPONIBLE AL PÚBLICO .....	78
2.2.5.10	MONITOREO.....	80
2.2.5.10.1	REGISTRO DE AUDITORÍAS.....	80
2.2.5.10.2	MONITOREO DE USO DEL SISTEMA.....	81
2.2.5.10.3	PROTECCIÓN DEL REGISTRO DE LA INFORMACIÓN .....	84
2.2.5.10.4	REGISTROS DEL ADMINISTRADOR Y DEL OPERADOR .....	85
2.2.5.10.5	REGISTRO DE FALLAS.....	85
2.2.5.10.6	SINCRONIZACIÓN DE RELOJES.....	86
2.2.6	CONTROL DEL ACCESO .....	87
2.2.6.1	REQUISITOS DEL NEGOCIO PARA EL CONTROL DEL ACCESO.....	87
2.2.6.1.1	POLÍTICA DE CONTROL DE ACCESO .....	88
2.2.6.2	GESTIÓN DEL ACCESO DE USUARIOS.....	90
2.2.6.2.1	REGISTRO DE USUARIOS.....	90
2.2.6.2.2	GESTIÓN DE PRIVILEGIOS .....	92
2.2.6.2.3	GESTIÓN DE CONTRASEÑAS PARA USUARIOS.....	93
2.2.6.2.4	REVISIÓN DE LOS DERECHOS DE ACCESO DE LOS USUARIOS.....	94
2.2.6.3	RESPONSABILIDADES DE LOS USUARIOS .....	95

2.2.6.3.1	USO DE CONTRASEÑAS .....	96
2.2.6.3.2	EQUIPO DE USUARIO DESATENDIDO .....	97
2.2.6.3.3	POLÍTICA DE ESCRITORIO DESPEJADO Y DE PANTALLA DESPEJADA ...	98
2.2.6.4	CONTROL DE ACCESO A LAS REDES .....	100
2.2.6.4.1	POLÍTICA DE USO DE LOS SERVICIOS EN RED .....	100
2.2.6.4.2	AUTENTICACIÓN DE USUARIOS PARA CONEXIONES EXTERNAS .....	101
2.2.6.4.3	IDENTIFICACIÓN DE LOS EQUIPOS EN LAS REDES .....	103
2.2.6.4.4	PROTECCIÓN DE LOS PUERTOS DE CONFIGURACIÓN Y DIAGNÓSTICO REMOTO .....	103
2.2.6.4.5	SEPARACIÓN EN LAS REDES.....	104
2.2.6.4.6	CONTROL DE CONEXIÓN A LAS REDES .....	106
2.2.6.4.7	CONTROL DEL ENRUTAMIENTO EN LA RED .....	107
2.2.6.5	CONTROL DE ACCESO AL SISTEMA OPERATIVO .....	108
2.2.6.5.1	PROCEDIMIENTOS DE REGISTRO DE INICIO SEGURO .....	108
2.2.6.5.2	IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS.....	110
2.2.6.5.3	SISTEMA DE GESTIÓN DE CONTRASEÑAS .....	112
2.2.6.5.4	USO DE LAS UTILIDADES DEL SISTEMA CONTROL.....	113
2.2.6.5.5	TIEMPO DE INACTIVIDAD DE LA SESIÓN .....	114
2.2.6.5.6	LIMITACIÓN DEL TIEMPO DE CONEXIÓN .....	115
2.2.6.6	CONTROL DE ACCESO A LAS APLICACIONES Y A LA INFORMACIÓN.....	115
2.2.6.6.1	RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN.....	116
2.2.6.6.2	AISLAMIENTO DE SISTEMAS SENSIBLES .....	117
2.2.6.7	COMPUTACIÓN MÓVIL Y TRABAJO REMOTO .....	118
2.2.6.7.1	COMPUTACIÓN Y COMUNICACIONES MÓVILES .....	118
2.2.6.7.2	TRABAJO REMOTO.....	120
2.2.7	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN .....	123
2.2.7.1	REQUISITOS DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN .	123
2.2.7.1.1	ANÁLISIS Y ESPECIFICACIÓN DE LOS REQUISITOS DE LA SEGURIDAD.... .....	123

2.2.7.2 PROCESAMIENTO CORRECTO EN LAS APLICACIONES .....	125
2.2.7.2.1 VALIDACIÓN DE LOS DATOS DE ENTRADA .....	125
2.2.7.2.2 CONTROL DE PROCESAMIENTO INTERNO .....	126
2.2.7.3 INTEGRIDAD DEL MENSAJE .....	128
2.2.7.3.1 VALIDACIÓN DE LOS DATOS DE SALIDA.....	129
2.2.7.4 CONTROLES CRIPTOGRÁFICOS.....	130
2.2.7.4.1 POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS.....	130
2.2.7.4.2 GESTIÓN DE CLAVES.....	132
2.2.7.5 SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA .....	134
2.2.7.5.1 CONTROL DEL SOFTWARE OPERATIVO.....	135
2.2.7.5.2 PROTECCIÓN DE LOS DATOS DE PRUEBA DEL SISTEMA .....	137
2.2.7.5.3 CONTROL DE ACCESO AL CÓDIGO FUENTE DE LOS PROGRAMAS .....	138
2.2.7.6 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE .....	139
2.2.7.6.1 PROCEDIMIENTOS DE CONTROL DE CAMBIOS .....	139
2.2.7.6.2 REVISIÓN TÉCNICA DE LAS APLICACIONES DESPUÉS DE LOS CAMBIOS EN EL SISTEMA OPERATIVO .....	141
2.2.7.6.3 RESTRICCIONES EN LOS CAMBIOS A LOS PAQUETES DE SOFTWARE	142
2.2.7.6.4 FUGA DE INFORMACIÓN.....	143
2.2.7.6.5 DESARROLLO DE SOFTWARE CONTRATADO EXTERNAMENTE .....	144
2.2.7.7 GESTIÓN DE LA VULNERABILIDAD TÉCNICA.....	145
2.2.7.7.1 CONTROL DE LAS VULNERABILIDADES TÉCNICAS.....	145
2.2.8 GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN...	148
2.2.8.1 REPORTE SOBRE LOS EVENTOS Y LAS DEBILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN .....	148
2.2.8.1.1 REPORTE SOBRE LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN .. .....	148
2.2.8.1.2 REPORTE SOBRE LAS DEBILIDADES EN LA SEGURIDAD .....	150
2.2.8.2 GESTIÓN DE LOS INCIDENTES Y LAS MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN .....	151
2.2.8.2.1 RESPONSABILIDADES Y PROCEDIMIENTOS.....	152



2.2.8.2.2 APRENDIZAJE DEBIDO A LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN .....	154
2.2.8.2.3 RECOLECCIÓN DE EVIDENCIAS .....	155
2.2.9 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO .....	157
2.2.9.1 ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO .....	157
2.2.9.1.1 INCLUSIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN EL PROCESO DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO .....	158
2.2.9.1.2 CONTINUIDAD DEL NEGOCIO Y EVALUACIÓN DE RIESGOS .....	159
2.2.9.1.3 DESARROLLO E IMPLEMENTACIÓN DE PLANES DE CONTINUIDAD QUE INCLUYAN LA SEGURIDAD DE LA INFORMACIÓN .....	160
2.2.9.1.4 ESTRUCTURA PARA LA PLANIFICACIÓN DE LA CONTINUIDAD DEL NEGOCIO.....	162
2.2.9.1.5 PRUEBAS, MANTENIMIENTO Y REEVALUACIÓN DE LOS PLANES DE CONTINUIDAD DEL NEGOCIO .....	164
2.2.10 CUMPLIMIENTO.....	166
2.2.10.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES.....	166
2.2.10.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE .....	166
2.2.10.1.2 DERECHOS DE PROPIEDAD INTELECTUAL (DPI).....	167
2.2.10.1.3 PROTECCIÓN DE LOS REGISTROS DE LA ORGANIZACIÓN.....	169
2.2.10.1.4 PROTECCIÓN DE LOS DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL .....	170
2.2.10.1.5 PREVENCIÓN DEL USO INADECUADO DE LOS SERVICIOS DE PROCESAMIENTO DE INFORMACIÓN .....	171
2.2.10.1.6 REGLAMENTACIÓN DE LOS CONTROLES CRIPTOGRÁFICOS.....	173
2.2.10.2 CUMPLIMIENTO DE LAS POLÍTICAS Y LAS NORMAS DE LA SEGURIDAD Y CUMPLIMIENTO TÉCNICO .....	174
2.2.10.2.1 CUMPLIMIENTO CON LAS POLÍTICAS Y LAS NORMAS DE LA SEGURIDAD .....	174
2.2.10.2.2 VERIFICACIÓN DEL CUMPLIMIENTO TÉCNICO.....	175

2.2.10.3 CONSIDERACIONES DE LA AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN .....	176
2.2.10.3.1 CONTROLES DE AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN.....	176
2.2.10.3.2 PROTECCIÓN DE LAS HERRAMIENTAS DE AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN .....	177
CAPÍTULO III.....	179
3 MANUAL DE POLÍTICAS DE SEGURIDAD.....	179
3.1 ACTIVOS.....	179
3.1.1 DE INFORMACIÓN .....	179
3.1.2 DE SOFTWARE, FÍSICOS Y SERVICIOS.....	180
3.2 EQUIPOS DE CÓMPUTO .....	181
3.2.1 DE LA INSTALACIÓN .....	181
3.2.2 PARA EL MANTENIMIENTO.....	183
3.2.3 DE LA ACTUALIZACIÓN.....	183
3.2.4 DE LA RE-UBICACIÓN .....	184
3.2.5 DE LA SEGURIDAD .....	184
3.3 COMUNICACIONES Y OPERACIONES.....	186
3.3.1 PROCEDIMIENTOS Y RESPONSABILIDADES.....	186
3.3.2 PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA.....	186
3.3.3 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS Y MÓVILES .....	187
3.3.4 RESPALDO .....	187
3.3.5 SEGURIDAD EN LAS REDES.....	188
3.3.6 MANEJO DE LOS MEDIOS.....	188
3.3.7 MONITOREO .....	188
3.4 CONTROL DE ACCESO .....	189
3.4.1 GESTIÓN DEL ACCESO DE LOS USUARIOS .....	189
3.4.2 RESPONSABILIDAD DE LOS USUARIOS.....	190
3.4.3 A LAS REDES .....	192
3.4.4 AL SISTEMA OPERATIVO, LAS APLICACIONES, INFORMACIÓN .....	192
3.4.5 COMPUTACIÓN MÓVIL Y TRABAJO REMOTO.....	193

3.4.6 A LA WEB.....	193
3.5 SOFTWARE .....	194
3.5.1 DE LA ADQUISICIÓN.....	194
3.5.2 DE LA INSTALACIÓN .....	195
3.5.3 DE LA ACTUALIZACIÓN.....	196
3.5.4 DE LA AUDITORIA DE SOFTWARE INSTALADO .....	196
3.5.5 DEL SOFTWARE PROPIEDAD DE LA INSTITUCIÓN.....	196
3.5.6 DE LA PROPIEDAD INTELECTUAL .....	197
3.6 INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN.....	197
3.6.1 REPORTE SOBRE LOS EVENTOS.....	198
3.6.2 REPORTE SOBRE LAS DEBILIDADES.....	198
3.6.3 GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN .....	199
3.7 SUPERVISIÓN Y CUMPLIMIENTO.....	199
3.7.1 CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD.....	199
3.7.2 VERIFICACIÓN DEL CUMPLIMIENTO TÉCNICO .....	200
3.7.3 CONSIDERACIONES DE LA AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN .....	200
CAPÍTULO IV .....	201
4 CONCLUSIONES Y RECOMENDACIONES .....	201
4.1 CONCLUSIONES .....	201
4.2 RECOMENDACIONES.....	202
BIBLIOGRAFÍA.....	203
ANEXOS.....	205
MANUAL DE POLÍTICAS DE SEGURIDAD EMELNORTE.....	205

## ÍNDICE DE GRÁFICOS

ILUSTRACIÓN 1: Estructura orgánica de la empresa.....	2
ILUSTRACIÓN 2: Amenazas .....	8
ILUSTRACIÓN 3: Política de Seguridad: Procesos, Reglas y Norma Institucionales .....	10

# **CAPÍTULO I**

## **1 INTRODUCCIÓN**

### **1.1 ANTECEDENTES**

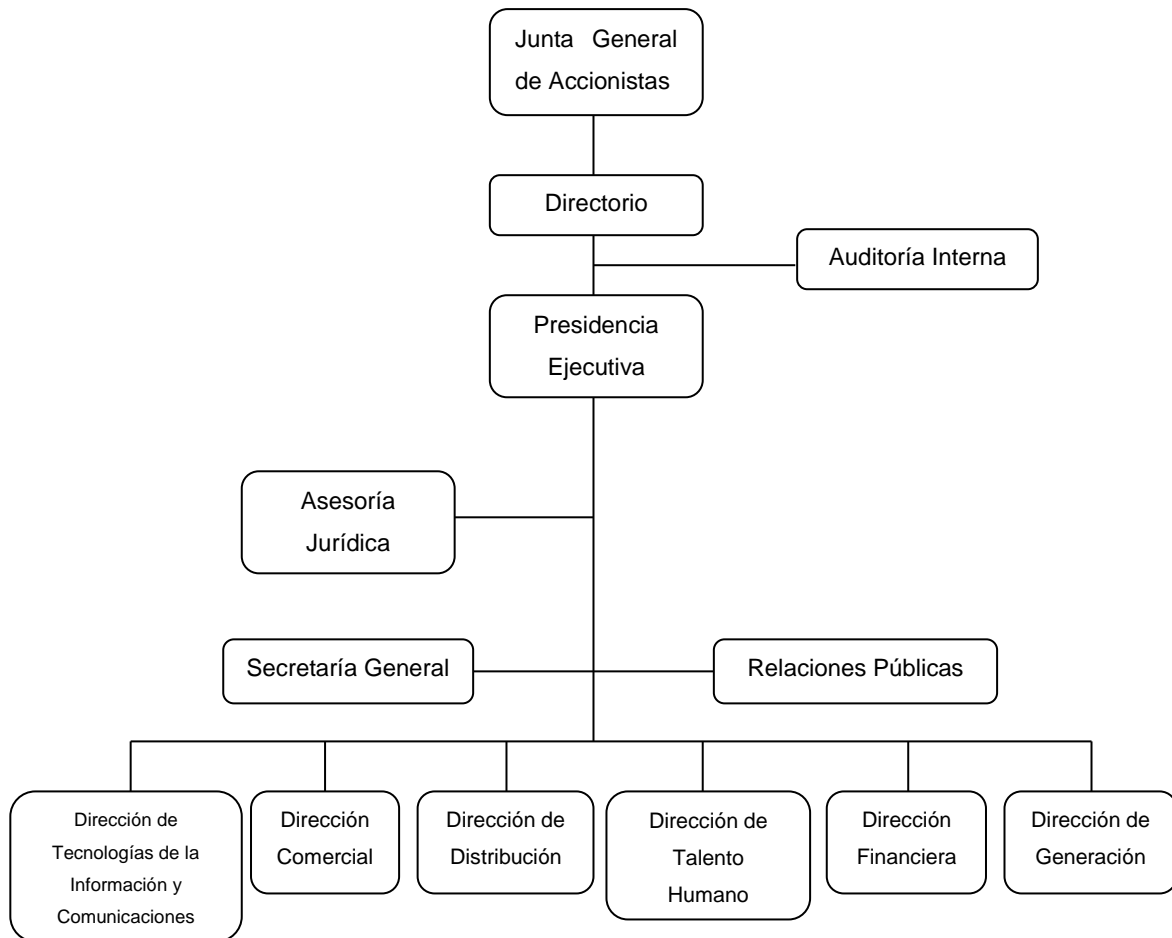
#### **1.1.1 MISIÓN**

Generar, distribuir y comercializar energía eléctrica bajo estándares de calidad para satisfacer las necesidades de sus clientes, con servicios de excelencia, personal calificado y comprometido, contribuyendo al desarrollo del país.

#### **1.1.2 VISIÓN**

EMELNORTE, será una empresa competitiva, técnica, moderna, modelo y referente del sector eléctrico, por la calidad de sus productos y servicios, gestión transparente y por su efectiva contribución al desarrollo del país.

### 1.1.3 ORGANIZACIÓN DE LA EMPRESA



**ILUSTRACIÓN 1:** Estructura orgánica de la empresa  
**Fuente:** EMELNORTE S.A.

## 1.2 PROBLEMA

La Empresa Eléctrica Regional Norte S.A. – EMELNORTE, es una empresa que posee una red de comunicaciones que integra a todos los usuarios que manejan equipos de computación. Es indispensable contar con políticas de seguridad que ayuden a desarrollar de mejor manera las actividades de intercambio de información y uso de sistemas.

Actualmente existen pocas políticas internas de seguridad, lo que ocasiona muchos inconvenientes en toda el área de concesión de EMELNORTE, tanto en los sistemas, comunicaciones, equipos de computación y la causa de malestar tanto a los abonados como a los usuarios de los sistemas de la empresa. Por ejemplo, la instalación de programas no permitidos en los equipos como los proxy que pueden crear huecos de seguridad en la red o el cambio de lugar de equipos sin previo conocimiento y autorización del Centro de Cómputo lo que causa errores en los registros e inventarios de equipos.

Por lo antes mencionado se ve imperiosa la necesidad de elaborar e implementar políticas y normas de seguridad basándose para su desarrollo en las NORMAS ISO.

## **1.3 OBJETIVOS**

### **1.3.1 OBJETIVO GENERAL**

Implementar las Políticas y Normas de Seguridad Informática para la Empresa Eléctrica Regional Norte S.A. – EMELNORTE.

### **1.3.2 OBJETIVOS ESPECÍFICOS**

1. Identificar los riesgos informáticos que enfrenta la empresa así como sus posibles consecuencias.
2. Proporcionar las reglas y procedimientos que deben implementarse para afrontar los riesgos identificados en los diferentes departamentos de la organización.
3. Detectar las vulnerabilidades del sistema de información para emitir las sugerencias y procedimientos respectivos para corregir estas falencias en las aplicaciones.
4. Aplicar la Norma Técnica Ecuatoriana INEN-ISO/IEC 27002:2009 para la elaboración del Manual de Políticas y Normas de Seguridad Informática para EMELNORTE.

## **1.4 JUSTIFICACIÓN**

Ante el esquema de globalización de la tecnologías de la información han originado principalmente por el uso masivo y universal de la internet y sus tecnologías, las instituciones se ven inmersas en ambientes agresivos donde el delinquir, sabotear y robar se convierte en retos para delincuentes informáticos universales conocidos como Hackers, Crackers, etc., es decir, en transgresores.

Conforme las tecnologías se han esparcido, la severidad y frecuencia las han transformado en un continuo riesgo, que obliga a las entidades a crear medidas de emergencia y políticas definitivas para contrarrestar estos ataques y transgresiones.

En nuestro país existen muchas instituciones que han sido víctimas de ataques en sus instalaciones, tanto desde el interior como del exterior, por lo que es necesario tratar de contrarrestar y anular estas amenazas reales.

Así pues, ante este panorama surge el proyecto de políticas rectoras que harán que el departamento de Tecnologías de la Información y la Comunicación de EMELNORTE, pueda disponer de los ejes de proyección que en materia de seguridad informática la institución requiere.

## **1.5 ALCANCE**

El resultado de la investigación es proveer a EMELNORTE de un manual que contendrá las políticas y normativas de seguridad informática.

Este manual de políticas de seguridad será elaborado de acuerdo al análisis de riesgos y de vulnerabilidades de EMELNORTE, por consiguiente el alcance de estas políticas se encuentra sujeto a la empresa. El contenido de dicho manual de políticas es el siguiente:

1. Antecedentes
2. Introducción



3. Políticas y Normas de Seguridad
  - 3.1. Activos
    - 3.1.1. De información
    - 3.1.2. De software
    - 3.1.3. Físicos
    - 3.1.4. Servicios
  - 3.2. Equipos de cómputo
    - 3.2.1. De la instalación
    - 3.2.2. Para el mantenimiento
    - 3.2.3. De la actualización
    - 3.2.4. De la re – ubicación
    - 3.2.5. De la seguridad
  - 3.3. Comunicaciones y operaciones
    - 3.3.1. Procedimientos y responsabilidades
    - 3.3.2. Planificación y aceptación del sistema
    - 3.3.3. Protección contra códigos maliciosos y móviles
    - 3.3.4. Respaldo
    - 3.3.5. Seguridad en las redes
    - 3.3.6. Manejo de los medios
    - 3.3.7. Monitoreo
  - 3.4. Control de acceso
    - 3.4.1. Gestión del acceso de los usuarios
    - 3.4.2. Responsabilidad de los usuarios
    - 3.4.3. A las redes
    - 3.4.4. Al sistema operativo, las aplicaciones, información
    - 3.4.5. Computación móvil y trabajo remoto
    - 3.4.6. A la web
  - 3.5. Software
    - 3.5.1. De la adquisición
    - 3.5.2. De la instalación
    - 3.5.3. De la actualización
    - 3.5.4. De la auditoria de software instaladores
    - 3.5.5. Del software propiedad de la institución
    - 3.5.6. De la propiedad intelectual
  - 3.6. Incidentes de la seguridad de la información
    - 3.6.1. Reporte sobre los eventos
    - 3.6.2. Reporte sobre las debilidades

- 3.6.3. Gestión de incidentes y mejoras en la seguridad de la información
- 3.7. Supervisión y cumplimiento
  - 3.7.1. Cumplimiento de las políticas y normas de seguridad
  - 3.7.2. Verificación del cumplimiento técnico
  - 3.7.3. Consideraciones de la auditoría de los sistemas de información
- 4. Referencias
- 5. Glosario

## CAPÍTULO II

### 2 MARCO TEÓRICO

#### 2.1 DEFINICIÓN DE LA SEGURIDAD INFORMÁTICA

##### 2.1.1 SEGURIDAD INFORMÁTICA

La seguridad informática se enfoca en la protección de la infraestructura computacional y todo lo relacionado. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

Consiste en garantizar que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.

Los objetivos de la seguridad informática se enfocan en:

**Integridad:** Certificar que los datos sean los que se supone que son.

**Confidencialidad:** Asegurar la disponibilidad de los recursos únicamente a los individuos autorizados.

**Disponibilidad:** Garantizar el correcto funcionamiento de los sistemas de información.

**Evitar el rechazo:** Garantizar de que no pueda negar una operación realizada.

**Autenticación:** Asegurar que sólo los individuos autorizados tengan acceso a los recursos.

## 2.1.2 AMENAZAS

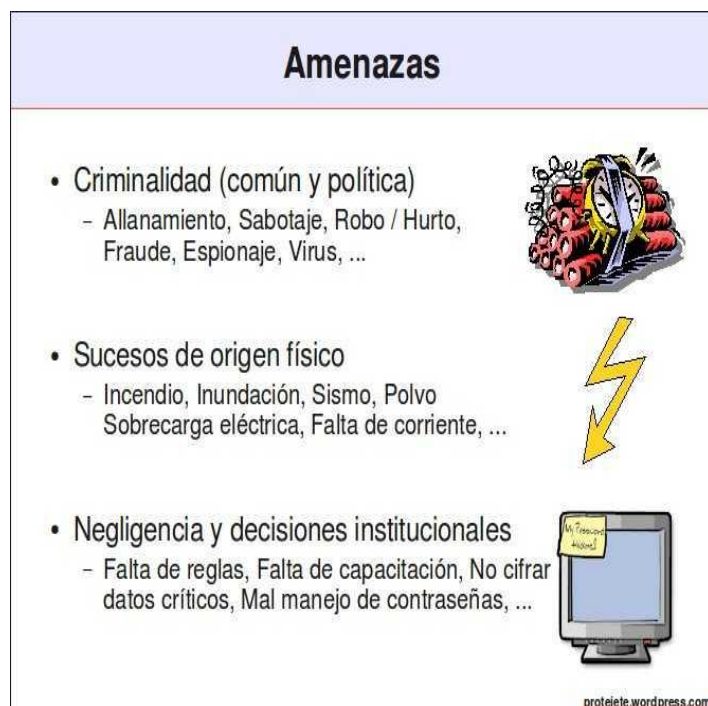


ILUSTRACIÓN 2: Amenazas

Una Amenaza, en el entorno informático, puede ser cualquier elemento que comprometa al sistema. Pueden presentarse circunstancias "no informáticas" que pueden afectar a los datos, las cuales son a menudo imprevisibles o inevitables.

Estos fenómenos pueden ser causados por:

**El usuario:** Causa del mayor problema ligado a la seguridad de un sistema informático (porque no le importa, no se da cuenta o a propósito).

**Programas maliciosos:** Programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en el ordenador abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica o un programa espía o Spyware.

**Un intruso:** Persona que consigue acceder a los datos o programas de los cuales no tiene acceso permitido (cracker, defacer, script kiddie o Script boy, viruxer, etc.).

**Un siniestro (robo, incendio, inundación):** Una mala manipulación o una mal intención derivan a la pérdida del material o de los archivos.

**El personal interno del Sistema:** Las pujas de poder que llevan a disociaciones entre los sectores y soluciones incompatibles para la seguridad informática.

### **2.1.3 ANÁLISIS DE RIESGOS**

La información es lo más importante dentro de una compañía y, por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo.

Los medios para conseguirlo son:

1. Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.
2. Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).
3. Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.
4. Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.
5. Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.
6. Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.
7. Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo.

Después de efectuar el análisis debemos determinar las acciones a tomar respecto a los riesgos residuales que se identificaron. Las acciones pueden ser:

**Controlar el riesgo.-** Fortalecer los controles existentes y/o agregar nuevos controles.

**Eliminar el riesgo.**- Eliminar el activo relacionado y con ello se elimina el riesgo.

**Compartir el riesgo.**- Mediante acuerdos contractuales parte del riesgo se traspasa a un tercero.

**Aceptar el riesgo.**- Se determina que el nivel de exposición es adecuado y por lo tanto se acepta.

## 2.1.4 POLÍTICAS DE SEGURIDAD



**ILUSTRACIÓN 3:** Política de Seguridad: Procesos, Reglas y Norma Institucionales

Generalmente se ocupa exclusivamente a asegurar los derechos de acceso a los datos y recursos con las herramientas de control y mecanismos de identificación. Estos mecanismos permiten saber que los operadores tienen sólo los permisos que se les dio.

La seguridad informática debe ser estudiada para que no impida el trabajo de los operadores en lo que les es necesario y que puedan utilizar el sistema informático con toda confianza. Por eso en lo referente a elaborar una política de seguridad, conviene:

- Elaborar reglas y procedimientos para cada servicio de la organización.

- Definir las acciones a emprender y elegir las personas a contactar en caso de detectar una posible intrusión
- Sensibilizar a los operadores con los problemas ligados con la seguridad de los sistemas informáticos.

Los derechos de acceso de los operadores deben ser definidos por los responsables jerárquicos y no por los administradores informáticos, los cuales tienen que conseguir que los recursos y derechos de acceso sean coherentes con la política de seguridad definida. Además, como el administrador suele ser el único en conocer perfectamente el sistema, tiene que derivar a la directiva cualquier problema e información relevante sobre la seguridad, y eventualmente aconsejar estrategias a poner en marcha, así como ser el punto de entrada de la comunicación a los trabajadores sobre problemas y recomendaciones en términos de seguridad informática.

### **2.1.5 RESPALDO**

La información constituye puede verse afectada por muchos factores tales como robos, incendios, fallas de disco, virus u otros. Desde el punto de vista de la empresa, uno de los problemas más importantes que debe resolver es la protección permanente de su información crítica.

La medida más eficiente para la protección de los datos es determinar una buena política de copias de seguridad o backups: Este debe incluir copias de seguridad completa (los datos son almacenados en su totalidad la primera vez) y copias de seguridad incrementales (sólo se copian los ficheros creados o modificados desde el último backup). Es vital para las empresas elaborar un plan de backup en función del volumen de información generada y la cantidad de equipos críticos.

Un buen sistema de respaldo debe contar con ciertas características indispensables:

**Continuo:** El respaldo de datos debe ser completamente automático y continuo. Debe funcionar de forma transparente, sin intervenir en las tareas que se encuentra realizando el usuario.

**Seguro:** Muchos software de respaldo incluyen cifrado de datos (128-448 bits), lo cual debe ser hecho localmente en el equipo antes del envío de la información.

**Remoto:** Los datos deben quedar alojados en dependencias alejadas de la empresa.

**Mantenimiento de versiones anteriores de los datos:** Se debe contar con un sistema que permita la recuperación de versiones diarias, semanales y mensuales de los datos.

## **2.2 NORMA TÉCNICA ECUATORIANA INEN-ISO/IEC 27002:2009**

### **2.2.1 EVALUACIÓN Y TRATAMIENTO DE RIESGOS**

#### **2.2.1.1 EVALUACIÓN DE LOS RIESGOS DE SEGURIDAD**

Una evaluación de riesgos debería identificar, cuantificar y priorizar los riesgos frente a los criterios para la aceptación del riesgo y los objetivos pertinentes para la organización.

Los resultados deberían guiar y determinar la acción de gestión adecuada y las prioridades tanto para la gestión de los riesgos de la seguridad de la información como para implementar los controles seleccionados para la protección contra estos riesgos.

Puede ser necesario llevar a cabo el proceso de evaluación de los riesgos y la selección de controles varias veces para cubrir diferentes partes de la organización o sistemas individuales de información.

Es recomendable que una evaluación de riesgos incluya el enfoque sistemático para estimar la magnitud de los riesgos (análisis del riesgo) y el proceso de comparación de los riesgos estimados frente a los criterios de riesgo para determinar la importancia de los riesgos (valoración del riesgo).



Es conveniente realizar periódicamente las evaluaciones de riesgos para abordar los cambios en los requisitos de la seguridad y en la situación de riesgo, por ejemplo en activos, amenazas, vulnerabilidades, impactos, valoración del riesgo y cuando se producen cambios significativos.

Estas evaluaciones de riesgos se deberían efectuar de forma metódica que puedan producir resultados comparables y reproducibles.

Una evaluación de los riesgos de la seguridad de la información debería tener un alcance definido claramente para que sea eficaz y debería incluir las relaciones con las evaluaciones de riesgos en otras áreas, según sea apropiado.

El alcance de una evaluación de riesgos puede abarcar a toda la organización, partes de la organización, un sistema individual de información, componentes específicos del sistema o servicios, cuando es factible, realista y útil.

#### **2.2.1.2 TRATAMIENTO DE LOS RIESGOS DE LA SEGURIDAD**

Antes de considerar el tratamiento de un riesgo, la organización debería decidir los criterios para determinar si se pueden aceptar o no los riesgos. Los riesgos se pueden aceptar si, por ejemplo, según una evaluación se considera el riesgo bajo o que el costo del tratamiento no es efectivo en términos financieros para la organización. Tales decisiones se deberían registrar.

Para cada uno de los riesgos identificados después de una evaluación de riesgos es necesario tomar una decisión para su tratamiento. Las opciones posibles para el tratamiento del riesgo incluyen:

- a) Aplicación de los controles apropiados para reducir los riesgos.
- b) Aceptación objetiva y con conocimiento de los riesgos, siempre y cuando ellos satisfagan la política de la organización y sus criterios para la aceptación del riesgo.
- c) Prevención de los riesgos al no permitir acciones que pudieran hacer que éstos se presentaran.

- d) Transferencia de riesgos asociados a otras partes, por ejemplo aseguradores o proveedores.

Para aquellos riesgos en donde la decisión de tratamiento del riesgo ha sido la aplicación de controles apropiados, dichos controles se deberían seleccionar e implementar de modo que satisfagan los requisitos identificados por una evaluación de riesgos.

Los controles deberían garantizar la reducción de los riesgos hasta un nivel aceptable teniendo en cuenta los siguientes elementos:

- a) Requisitos y restricciones de la legislación y de las regulaciones nacionales e internacionales.
- b) Objetivos de la organización.
- c) Requisitos y restricciones operativas.
- d) Costo de la implementación y la operación con relación a la reducción de los riesgos, y que se mantenga proporcional a los requisitos y restricciones de la organización.
- e) Necesidad de equilibrar la inversión en la implementación y operación de los controles frente a la probabilidad del daño que resultara debido a las fallas de seguridad.

Los controles se pueden seleccionar a partir de esta norma, de otros conjuntos de controles, o se puede diseñar controles nuevos que satisfagan las necesidades específicas de la organización. Es necesario reconocer que es posible que algunos controles no se puedan aplicar a todos los sistemas y entornos de la información, y pueden no ser viables para todas las organizaciones.

Los controles de la seguridad de la información se deberían tener en cuenta en la especificación de los requisitos de sistemas y proyectos y en la fase de diseño. De lo contrario, se pueden originar costos adicionales y soluciones menos eficaces y, es posible, en el peor de los casos, la incapacidad de lograr una seguridad adecuada.

## **2.2.2 POLÍTICA DE LA SEGURIDAD**

El objetivo es brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.

Las directivas deberían establecer una dirección clara de la política según los objetivos del negocio y demostrar apoyo y compromiso con la seguridad de la información a través de la emisión y el mantenimiento de la política de la seguridad de la información en toda organización.

### **2.2.2.1 DOCUMENTO DE LA POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN**

#### **Control**

La dirección debería aprobar un documento de política de la seguridad de la información y lo debería publicar y comunicar a todos los empleados y partes externas pertinentes.

#### **Guía de implementación**

El documento de la política de la seguridad de la información debería declarar el compromiso de la dirección y establecer el enfoque de ésta para la gestión de la seguridad de la información. El documento de la política debería contener declaraciones relacionadas con:

- a) Una definición de la seguridad de la información, sus objetivos generales y el alcance e importancia de la seguridad como mecanismo que permite compartir la información.
- b) Una declaración de la intención de la dirección, que apoye las metas y los principios de la seguridad de la información, de acuerdo con la estrategia y los objetivos del negocio.
- c) Un marco referencial para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación de riesgos y de la gestión del riesgo.

- d) Una explicación breve sobre las políticas, los principios, las normas de la seguridad, así como de los requisitos de cumplimiento de importancia particular para la organización incluyendo los siguientes:
  - a. Cumplimiento de los requisitos legales, reglamentarios y contractuales.
  - b. Requisitos de educación, formación y concienciación sobre la seguridad.
  - c. Gestión de la continuidad del negocio.
  - d. Consecuencias de las violaciones de la política de la seguridad.
  
- e) Definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información, incluyendo el reporte de los incidentes de la seguridad de la información.
  
- f) Referencias a la documentación que puede dar soporte a la política, por ejemplo políticas de la seguridad más detalladas y procedimientos para sistemas específicos de información o las reglas de la seguridad que deberían cumplir los usuarios.

Esta política de la seguridad de la información se debería comunicar a través de toda la organización a los usuarios de manera pertinente, accesible y comprensible para el lector.

### **Información adicional**

La política de la seguridad de la información podría formar parte de un documento de política general. Si la política de la seguridad de la información se distribuye fuera de la organización, es necesario tener cuidado de no divulgar información sensible.

### **2.2.2.2 REVISIÓN DE LA POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN**

#### **Control**

La política de la seguridad de la información se debería revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada suficiente y eficaz.

## Guía de implementación

La política de la seguridad de la información debería tener un responsable aprobado por la dirección para el desarrollo, la revisión y la valoración de dicha política.

Es conveniente que la revisión incluya las oportunidades de evaluación para mejorar la política de la seguridad de la información de la organización y el enfoque para la gestión de la seguridad de la información en respuesta a los cambios en el entorno de la organización, las circunstancias del negocio, las condiciones legales o el entorno técnico.

Es conveniente que la revisión de la política de la seguridad de la información tenga en cuenta los resultados de la revisión por la dirección. Deberían existir procedimientos definidos para la revisión por la dirección, incluyendo una programación o periodo de revisión.

Las entradas para la revisión por la dirección deberían incluir información sobre:

- a) Retroalimentación de las partes interesadas.
- b) Resultados de las revisiones independientes.
- c) Estados de las acciones preventivas y correctivas.
- d) Resultados de las revisiones previas por parte de la dirección.
- e) Desempeño del proceso y cumplimiento de la política de la seguridad de la información.
- f) Cambios que pudieran afectar el enfoque de la organización para la gestión de la seguridad de la información, incluyendo cambios en el entorno de la organización, las circunstancias del negocio, la disponibilidad de recursos, las condiciones contractuales, reglamentarias o legales, o el entorno técnico.
- g) Tendencias relacionadas con las amenazas y las vulnerabilidades.
- h) Incidentes de la seguridad de la información reportados.

- i) Recomendaciones de las autoridades pertinentes.

Los resultados de la revisión por la dirección deberían incluir todas las decisiones y acciones relacionadas con:

- a) Mejora del enfoque de la organización para la gestión de la seguridad de la información y sus procesos.
- b) Mejora de los objetivos de control y de los controles.
- c) Mejora de la asignación de recursos y/o responsabilidades.

Es recomendable mantener un registro de la revisión por la dirección.

Se debería obtener la aprobación de la dirección para la política revisada.

## **2.2.3 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**

### **2.2.3.1 ORGANIZACIÓN INTERNA**

El objetivo es gestionar la seguridad de la información dentro de la organización.

Se debería establecer un marco referencial de gestión para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.

La dirección debería aprobar la política de la seguridad de la información, asignar las funciones de la seguridad, coordinar y revisar la implementación de la seguridad en toda la organización.

Si es necesario, se recomienda establecer una fuente de asesoría especializada sobre seguridad de la información y ponerla a disposición en la organización. Es conveniente desarrollar contactos con grupos o especialistas externos en seguridad, incluyendo las autoridades pertinentes, para ir al compás de las tendencias industriales, monitorear normas y métodos de evaluación, así como proveer puntos adecuados de vínculo cuando se manejan incidentes de la seguridad de la información. Se debería promover un enfoque multidisciplinario para la seguridad de la información.

### **2.2.3.1.1 COMPROMISO DE LA DIRECCIÓN CON LA SEGURIDAD DE LA INFORMACIÓN**

#### **Control**

La dirección debería apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explícita y el conocimiento de las responsabilidades de la seguridad de la información.

#### **Guía de implementación**

La dirección debería:

- a) Asegurar que las metas de la seguridad de la información están identificadas, satisfacen los requisitos de la organización y están integradas en los procesos pertinentes.
- b) Formular, revisar y aprobar la política de la seguridad de la información.
- c) Revisar la eficacia de la implementación de la política de la seguridad de la información.
- d) Proporcionar un rumbo claro y apoyo visible para las iniciativas de la seguridad.
- e) Proporcionar los recursos necesarios para la seguridad de la información.
- f) Aprobar la asignación de funciones y responsabilidades específicas para la seguridad de la información en toda la organización.
- g) Iniciar planes y programas para mantener la concienciación sobre la seguridad de la información.
- h) Asegurar la coordinación en toda la organización de la implementación de los controles de la seguridad de la información.

La dirección debería identificar las necesidades de asesoría especializada interna o externa sobre la seguridad de información, revisar y coordinar los resultados de la asesoría en toda la organización.

Dependiendo del tamaño de la organización, tales responsabilidades se podrían manejar a través de un comité de dirección dedicado a esta labor o a través de un organismo de dirección ya existente, como por ejemplo el consejo de directores.

### **2.2.3.1.2 COORDINACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**

#### **Control**

Las actividades de la seguridad de la información deberían ser coordinadas por los representantes de todas las partes de la organización con roles y funciones laborales pertinentes.

#### **Guía de implementación**

Comúnmente, la coordinación de la seguridad de la información involucra la cooperación y colaboración de directores, usuarios, administradores, diseñadores de aplicación, auditores y personal de seguridad, así como habilidades especializadas en áreas como seguros, temas legales, recursos humanos, tecnología de la información o gestión de riesgos.

Esta actividad debería:

- a) Garantizar que las actividades de la seguridad se efectúan en cumplimiento de la política de la seguridad de la información.
- b) Identificar la forma de manejar los no cumplimientos.
- c) Aprobar metodologías y procesos para la seguridad de la información, como una evaluación de riesgos y la clasificación de información.



- d) Identificar cambios significativos de las amenazas y la exposición de la información y de los servicios de procesamiento de la información de las amenazas.
- e) Evaluar la idoneidad y coordinar la implementación de los controles de la seguridad de la información.
- f) Promover eficazmente la educación, la formación y la concienciación de la seguridad de la información en toda la organización.
- g) Valorar la información recibida del monitoreo y la revisión de los incidentes de la seguridad de la información, y recomendar las acciones apropiadas para responder a los incidentes identificados de la seguridad de la información.

Si la organización no emplea un grupo específico multifuncional, por ejemplo debido a que dicho grupo no es apropiado para el tamaño de la organización, las acciones descritas anteriormente las debería llevar a cabo otro organismo de la dirección o un solo director.

#### **2.2.3.1.3 ASIGNACIÓN DE RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN**

##### **Control**

Se deberían definir claramente todas las responsabilidades en cuanto a seguridad de la información.

## **Guía de implementación**

La asignación de responsabilidades para la seguridad de la información se debería realizar de acuerdo con la política de la seguridad de la información. Se recomienda definir claramente las responsabilidades para la protección de activos individuales y para la ejecución de procesos específicos de la seguridad. Esta responsabilidad debería complementarse, cuando es necesario, con directrices más detalladas para sitios específicos y servicios específicos de procesamiento de información. Se debería definir claramente las responsabilidades locales para la protección de activos y para realizar procesos específicos de la seguridad, como por ejemplo la planificación de la continuidad del negocio.

Los individuos con responsabilidades de la seguridad asignadas pueden delegar las labores de la seguridad a otros. No obstante, siguen siendo responsables y debería determinar la ejecución correcta de las labores delegadas.

Las áreas por las cuales son responsables los individuos se deberían establecer con claridad, en particular, se deberían establecer las siguientes:

Los activos y los procesos de la seguridad asociados con cada sistema particular se deberían identificar y definir claramente.

Se debería asignar la entidad responsable de cada activo o proceso de la seguridad, así como documentar esta responsabilidad.

Se deberían definir y documentar claramente los niveles de autorización.

### **Información adicional**

En muchas organizaciones se designará un director de la seguridad de la información con toda la responsabilidad por el desarrollo e implementación de la seguridad y para apoyar la identificación de controles.

Sin embargo, la responsabilidad por los recursos y la implementación de controles permanecerá en los directores individuales. Una práctica común es designar un responsable para cada activo, quien se hace responsable de su protección diaria.

#### **2.2.3.1.4 PROCESO DE AUTORIZACIÓN PARA LOS SERVICIOS DE PROCESAMIENTO DE LA INFORMACIÓN**

##### **Control**

Se debería definir e Implementar un proceso de autorización de la dirección para nuevos servicios de procesamiento de la Información.

##### **Guía de implementación**

Se recomienda tener en cuenta las siguientes directrices para el proceso de autorización:

- a) Los servicios nuevos deberían tener autorización de la dirección para el usuario apropiado, autorizando su propósito y uso. La autorización también se debería obtener del director responsable de mantener el entorno de la seguridad del sistema de Información local para asegurar el cumplimiento de todas las políticas y los requisitos de la seguridad correspondientes.
- b) Cuando es necesario, el hardware y el software se deberían verificar para asegurar que son compatibles con otros componentes del sistema.
- c) La utilización de servicios de procesamiento de Información personales o privados, por ejemplo computadores portátiles (laptops). computadores domésticos o dispositivos manuales para procesar información del negocio, pueden introducir nuevas vulnerabilidades y se deberían identificar e implementar los controles necesarios.

#### **2.2.3.1.5 ACUERDOS SOBRE CONFIDENCIALIDAD**

##### **Control**

Se deberían identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que reflejan las necesidades de la organización para la protección de la información.

## Guía de implementación

Los acuerdos de confidencialidad o de no-divulgación deberían abordar los requisitos para proteger la información confidencial usando términos que se puedan hacer cumplir legalmente.

Para identificar los requisitos para los acuerdos de confidencialidad o de no-divulgación, se deberían considerar los siguientes elementos:

- a) Definición de la información que se ha de proteger (por ejemplo la información confidencial).
- b) Duración esperada del acuerdo, incluyendo los casos en que puede ser necesario mantener la confidencialidad indefinidamente.
- c) Acciones requeridas cuando se termina un acuerdo.
- d) Responsabilidades y acciones de los que suscriben el acuerdo de confidencialidad para evitar la divulgación no autorizada de información (tal como "necesidad de conocer").
- e) Propiedad de la información, secretos comerciales y propiedad intelectual y cómo se relaciona con la protección de información confidencial.
- f) El uso permitido de la información confidencial y los derechos de los que suscriben el acuerdo de confidencialidad a usar la información.
- g) Derecho de auditar y monitorear las actividades que involucran a la información confidencial.
- h) Proceso para la notificación y el reporte de divulgación no autorizada o violación de la información confidencial.
- i) Términos para la devolución o la destrucción de la información al terminar el acuerdo.
- j) Acciones esperadas a tomar en caso de incumplimiento de este acuerdo.

Con base en los requisitos de la seguridad de la organización, pueden ser necesarios otros elementos en un acuerdo de confidencialidad o no-divulgación.

Los acuerdos de confidencialidad o no-divulgación deberían cumplir todas las leyes y las regulaciones que se aplican en la jurisdicción correspondiente.

Los requisitos para los acuerdos de confidencialidad o no- divulgación se deberían revisar periódicamente y cuando se produzcan cambios que influyan en estos requisitos.

### **Información adicional**

Los acuerdos de confidencialidad y de no-divulgación protegen la información de la organización e informan a los que suscriben el acuerdo de confidencialidad, sus responsabilidades para proteger, utilizar y divulgar información de forma responsable y autorizada.

Puede ser necesario que de la organización utilice diferentes formas de acuerdos de confidencialidad y de no-divulgación en circunstancias diferentes.

### **2.2.3.1.6 CONTACTO CON LAS AUTORIDADES**

#### **Control**

Se deberían mantener contactos apropiados con las autoridades pertinentes.

#### **Guía de implementación**

Las organizaciones deberían tener procedimientos establecidos que especifiquen cuándo y a través de que autoridades (policía, bomberos, autoridades de supervisión) se debería contactar y la forma en que se deberían reportar oportunamente los incidentes identificados de la seguridad de la información, si se sospecha de incumplimiento de la ley.

Puede que las organizaciones sometidas a ataques provenientes de Internet necesiten terceras partes externas (por ejemplo un proveedor de servicios de Internet o un operador de telecomunicaciones) para tomar acción contra la fuente de los ataques.

## **Información adicional**

El mantenimiento de dichos contactos puede ser un requisito para dar soporte a la gestión de incidentes de la seguridad de la información o a la continuidad del negocio y el proceso de planes de contingencia. Los contactos con los organismos de regulación también son útiles para anticipar y preparar los cambios futuros en la ley o en los reglamentos que la organización debe cumplir.

Los contactos con otras autoridades incluyen servicios públicos, servicios de emergencia, salud y seguridad, como el departamento de bomberos (en conexión con la continuidad del negocio), proveedores de telecomunicaciones (junto con enrutamiento de línea y disponibilidad) y proveedores de agua (junto con medios de refrigeración para los equipos).

### **2.2.3.1.7 CONTACTOS CON GRUPOS DE INTERÉS ESPECIALES**

#### **Control**

Se deberían mantener los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información, y asociaciones de profesionales.

#### **Guía de implementación**

La pertenencia a foros o grupos de interés especial se debería considerar un medio para:

- a) Mejorar el conocimiento sobre las mejores prácticas y estar actualizado con la información pertinente a la seguridad.
- b) Garantizar que la comprensión del entorno de la seguridad de la información es actual y completa.
- c) Recibir advertencias oportunas de alertas, avisos y parches relacionados con ataques y vulnerabilidades.
- d) Obtener acceso a asesoría especializada sobre seguridad de la información.

- e) Compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades.
- f) Suministrar puntos adecuados de enlace cuando se trata de incidentes de la seguridad de la información.

### **Información adicional**

Se pueden establecer acuerdos para compartir información con el objeto de mejorar la cooperación y la coordinación de los temas de la seguridad. Dichos acuerdos deberían identificar los requisitos para la protección de la Información sensible.

### **2.2.3.1.8 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN**

#### **Control**

El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados, o cuando ocurran cambios significativos en la implementación de la seguridad.

#### **Guía de implementación**

La dirección debería poner en marcha la revisión independiente. Esta revisión independiente es necesaria para asegurar la eficacia, idoneidad y propiedad del enfoque de la organización para la gestión de la seguridad de la información. La revisión debería incluir una evaluación de las oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad, incluyendo la política y los objetivos de control.

Dicha revisión debería ser realizada por personas independientes del área sometida a revisión, por ejemplo por la función de auditoría interna, un director independiente o de la organización de tercera parte especializada en tales revisiones. Los individuos que llevan a cabo estas revisiones deberían tener la experiencia y las habilidades adecuadas.

Se recomienda que los resultados de la revisión independiente se registren y se reporten a la dirección que ha iniciado la revisión. Estos registros se deberían conservar.

Si la revisión identifica que el enfoque y la implementación de la organización con respecto a la gestión del sistema de la seguridad son inadecuados o no cumplen la orientación para la seguridad de la información establecida en el documento de la política de la seguridad de la información, la dirección debería considerar las acciones correctivas.

### **Información adicional**

El área que los directores deberían revisar regularmente también se podría revisar independientemente. Las técnicas de revisión pueden incluir entrevistas de la dirección, verificación de registros o revisión de los documentos de la política de la seguridad. La norma NTE-INEN/ISO 19011:2002, Directrices para la auditoría de los sistemas de gestión ambiental y/o de calidad también puede suministrar una guía útil para llevar a cabo la revisión independiente, incluyendo el establecimiento y la implementación de un programa de revisión.

#### **2.2.3.2 PARTES EXTERNAS**

Mantener la seguridad de la información y de los servicios de procesamiento de información de la organización a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por éstas.

La seguridad de la información y de los servicios de procesamiento de información no se deberían reducir introduciendo productos o servicios de partes externas.

Se debería controlar todo acceso a los servicios de procesamiento de información no se deberían reducir introduciendo productos o servicios de partes externas.

Cuando existe una necesidad del negocio de trabajar con partes externas que pueden requerir acceso a la información de la organización y a sus servicios de procesamiento de información, o de obtener o suministrar productos y servicios de o para una parte externa, se debería realizar una evaluación de riesgos para determinar las implicaciones para la seguridad y los requisitos de control. Los controles se deberían acordar y definir en un convenio con la parte externa.



### **2.2.3.2.1 IDENTIFICACIÓN DE LOS RIESGOS RELACIONADOS CON LAS PARTES EXTERNAS**

#### **Control**

Se deberían identificar los riesgos para la información y los servicios de procesamiento de información de la organización en los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso.

#### **Guía de implementación**

Cuando existe la necesidad de permitir el acceso de una parte externa a los servicios de procesamiento de información o a la información de la organización, es recomendable llevar a cabo una evaluación de riesgos (véase también la sección 4) para identificar los requisitos para los controles específicos. En la identificación de los riesgos relacionados con el acceso de partes externas se deberían considerar los siguientes aspectos:

- a) Los servicios de procesamiento de información a los cuales requiere acceso la parte externa.
- b) El tipo de acceso que tendrá la parte externa a la información y a los servicios de procesamiento de información, por ejemplo:
  - a. Acceso físico, por ejemplo a oficinas, recintos de computadores y gabinetes de archivos.
  - b. Acceso lógico, por ejemplo a las bases de datos de la organización o a los sistemas de la organización.
  - c. Conexión de red entre las redes de la organización y de la parte externa por ejemplo conexión permanente, acceso remoto.
  - d. Si el acceso tendrá lugar en las instalaciones o fuera de ellas.
- c) El valor y la sensibilidad de la información involucrada y su importancia para las operaciones del negocio.

- d) Los controles necesarios para proteger la información que no está destinada a ser accesible por las partes externas.
- e) El personal de la parte externa involucrado en manejar la información de la organización.
- f) La forma en que se puede identificar a la organización o al personal autorizado a tener acceso, la manera de verificar la autorización, así como la forma en que es necesario confirmarlo.
- g) Los diferentes medios y controles utilizados por la parte externa al almacenar, procesar, comunicar, compartir e intercambiar la información.
- h) El impacto del acceso denegado a la parte externa cuando lo requiere y la recepción o el acceso de la parte externa a información inexacta o engañosa.
- i) Las prácticas y los procedimientos para tratar los incidentes de la seguridad de la información y los daños potenciales, al igual que los términos y las condiciones para la continuación del acceso de la parte externa en el caso de un incidente de la seguridad de la información.
- j) Los requisitos legales y reglamentarios y otras obligaciones contractuales pertinentes a la parte externa que se deberían tener en cuenta.
- k) La forma en que se podrían ver afectados los intereses de cualquier otro accionista debido a los acuerdos.

El acceso de las partes externas a la información de la organización no se debería brindar hasta haber implementado los controles apropiados y, cuando es viable, haber firmado un contrato que defina los términos y las condiciones para la conexión o el acceso y el acuerdo de trabajo. En general, todos los requisitos de la seguridad, que resultan del trabajo con partes externas, o los controles internos se deberían reflejar en el acuerdo con la parte externa.

Se debería garantizar que la parte externa es consciente de sus obligaciones y acepta las responsabilidades y deberes involucrados en el acceso, procesamiento, comunicación o gestión de la información y los servicios de procesamiento de información de la organización.

- a) Procedimientos para proteger los activos de la organización, incluyendo información, software y hardware.
- b) Todos los controles y mecanismos de protección física requeridos.
- c) Controles para asegurar la protección contra software malicioso.
- d) Procedimientos para determinar si alguna vez se han puesto en peligro los activos, por ejemplo pérdida o modificación de información. software y hardware.
- e) Controles para asegurar la devolución o la destrucción de la Información y los activos al finalizar el acuerdo o en un punto acordado en el tiempo durante la duración del acuerdo.
- f) Confidencialidad, Integridad, disponibilidad y cualquier otra propiedad pertinente de los activos.
- g) Restricciones a la copia y a la divulgación de información, y uso de acuerdos de confidencialidad.
- h) La formación del usuario y del administrador en métodos, procedimientos y seguridad.
- i) Asegurar la concienciación del usuario sobre responsabilidades y aspectos de La seguridad de la información.
- j) Las disposiciones para la transferencia de personal, cuando es apropiado.
- k) Las responsabilidades relacionadas con la instalación y el mantenimiento del software y el hardware.
- l) La estructura clara y los formatos acordados para la presentación de los informes.

- m) El proceso claro y específico para la gestión de cambios.
- n) La política de control del acceso, incluyendo:
  - a. Diversas razones, requisitos y beneficios de la necesidad del acceso por terceras partes.
  - b. Métodos de acceso permitido y control y uso de identificadores únicos, tales como las identificaciones de usuario (ID) y las contraseñas.
  - c. Proceso de autorización para los privilegios y el acceso del usuario.
  - d. Requisito para mantener una lista de las personas autorizadas a usar los servicios que se ponen a disposición, y de sus derechos y privilegios con relación a tal uso.
  - e. Declaración de que el acceso que no se autorice explícitamente esté prohibido.
  - f. Proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas.
- o) Las disposiciones para el reporte, la notificación y la investigación de los incidentes de seguridad de la Información y las violaciones de la seguridad, así como los incumplimientos de los requisitos establecidos en el acuerdo.
- p) Una descripción del producto o servicio que va a ser proporcionado y una descripción de la información que va a estar disponible junto con su clasificación de la seguridad.
- q) La meta del nivel de servicio y los niveles inaceptables de servicio.
- r) La definición de criterios verificables de desempeño, su monitoreo y reporte.
- s) El derecho a monitorear y revocar cualquier actividad relacionada con los activos de la organización.

- t) El derecho a auditar las responsabilidades definidas en el acuerdo, a que dichas auditorías sean realizadas por una tercera parte y a enumerar los derechos estatutarios de los auditores.
- u) El establecimiento de un proceso gradual para la solución de problemas.
- v) Los requisitos de la continuidad del servicio, incluyendo las medidas para la disponibilidad y confiabilidad, de acuerdo con las prioridades del negocio de la organización.
- w) Las responsabilidades civiles correspondientes de las partes del acuerdo.
- x) Las responsabilidades relacionadas con asuntos legales y la forma en que se garantiza el cumplimiento de los requisitos legales, por ejemplo la legislación sobre protección de datos, teniendo en cuenta particularmente los diversos sistemas legales nacionales, si el acuerdo implica cooperación con organizaciones en otros países.
- y) Los derechos de propiedad intelectual (DPI) y asignación de derechos de copia y la protección de cualquier trabajo colaborativo.
- z) La participación de la tercera parte con los subcontratistas y los controles de la seguridad que estos subcontratistas necesitan implementar.
- aa) Las condiciones para la renegociación / terminación del acuerdo:
  - a. Se debería establecer un plan de contingencia en caso de que cualquiera de las partes desee terminar la relación antes de la finalización de los acuerdos.
  - b. Renegociación de acuerdos si cambian los requisitos de la seguridad de la organización.
  - c. Documentación vigente de las listas de activos, licencias, acuerdos o derechos relacionados con ellos.

## **Información adicional**

Los acuerdos pueden variar considerablemente para diferentes organizaciones y entre los diferentes tipos de terceras partes. Por lo tanto, se debe tener cuidado al incluir todos los riesgos y requisitos de la seguridad identificados en los acuerdos.

Cuando es necesario, los procedimientos y controles requeridos se pueden ampliar en el plan de gestión de la seguridad.

Si la gestión de la seguridad se contrata externamente, los acuerdos deberían abarcar la forma en que la tercera parte garantizará la seguridad adecuada, tal como se definió mediante la evaluación de riesgos, cómo mantendrá la seguridad, y como se adaptará la seguridad para identificar y tratar los cambios en los riesgos.

Algunas de las diferencias entre la contratación externa y otras formas de prestación de servicios de terceras partes incluyen el tema de la responsabilidad civil, la planificación del periodo de transición y la interrupción potencial de las operaciones durante este periodo, acuerdos sobre planificación de contingencias y revisiones con la debida diligencia, así como la recolección y gestión de información sobre incidentes de la seguridad. Por ello, es importante que la organización planifique y gestione la transición hacia un acuerdo contratado externamente y tenga procesos adecuados establecidos para la gestión de los cambios y la renegociación / terminación de los acuerdos.

Es necesario considerar en el acuerdo los procedimientos para el procesamiento continuo, en el caso de que la tercera parte no pueda suministrar sus servicios, para evitar cualquier retraso en la provisión de los servicios de remplazo.

Los acuerdos con las partes externas también pueden involucrar a otras partes. Los acuerdos que otorgan acceso a la tercera parte deberían incluir la permisividad para la designación de otras partes y las condiciones elegibles para su acceso y participación.

En general, los acuerdos los desarrolla en primer término la organización. Puede haber ocasiones, en algunas circunstancias, en que una tercera parte pueda desarrollar un acuerdo e imponerlo a la organización. Es necesario que la organización garantice que su propia seguridad no sufra impactos innecesarios debido a los requisitos de la tercera parte estipulados en los acuerdos impuestos.

## **2.2.4 GESTIÓN DE ACTIVOS**

### **2.2.4.1 RESPONSABILIDAD POR LOS ACTIVOS**

Lograr y mantener la protección adecuada de los activos de la organización.

Todos los activos se deben incluir y deben tener un responsable designado.

Se debería identificar los responsables para todos los activos y asignar la responsabilidad para el mantenimiento de los controles adecuados. La implementación de los controles específicos puede ser delegada por el responsable, según el caso, pero él sigue siendo responsable, según el caso, pero él sigue siendo responsable de la protección adecuada de los activos.

#### **2.2.4.1.1 INVENTARIO DE ACTIVOS**

##### **Control**

Todos los activos deberían estar claramente identificados y se debería elaborar y mantener un inventario de todos los activos importantes.

##### **Guía de implementación**

La organización debería identificar todos los activos y documentar su importancia. El inventario de activos debería incluir toda la información necesaria para recuperarse de los desastres, incluyendo el tipo de activo, el formato, la ubicación, la información de soporte, la información sobre licencias y el valor para el negocio.

Este inventario no debería duplicar innecesariamente otros inventarios, pero se debería garantizar que el contenido esté acorde.

Además, se deberían acordar y documentar la propiedad y la clasificación de la información para cada uno de los activos. Con base en la importancia del activo, su valor para el negocio y su clasificación de la seguridad se recomienda identificar los niveles de protección según la importancia de los activos.

## Información adicional

Existen muchos tipos de activos, incluyendo:

- a) Información: bases de datos y archivos de datos, contratos y acuerdos, documentación del sistema, Información sobre investigación, manuales de usuario, material de formación, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos de recuperación, registros de auditoría e información archivada.
- b) Activos de software: software de aplicación, software del sistema, herramientas de desarrollo y utilidades.
- c) Activos físicos: equipos de computación, equipos de comunicaciones, medios removibles y otros equipos.
- d) Servicios: servicios de computación y comunicaciones, servicios generales como por ejemplo iluminación, calefacción, energía y aire acondicionado.
- e) Personas y sus calificaciones, habilidades y experiencia.
- f) Intangibles tales como reputación e imagen de la organización.

Los inventarios de activos ayudan a garantizar que se logra la protección eficaz de los activos y también se puede requerir para otros propósitos del negocio como por ejemplo por razones de salud y seguridad, financieras o de seguros (gestión de activos). El proceso para obtener un inventario de activos es un prerrequisito importante de la gestión de riesgos.



## 2.2.4.1.2 RESPONSABLE DE LOS ACTIVOS

### Control

Toda la información y los activos asociados con los servicios de procesamiento de información deberían ser asignada a una parte de la organización que actúa como responsable<sup>1</sup>.

### Guía de implementación

El responsable del activo debería responsabilizarse de:

- a) Garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente.
- b) Definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.

La responsabilidad puede ser designada para:

- a) Un proceso del negocio.
- b) Un conjunto definido de actividades.
- c) Una aplicación.
- d) Un conjunto definido de datos.

### Información adicional

Las labores rutinarias se pueden delegar, por ejemplo a un custodio que cuide el activo diariamente, pero la responsabilidad sigue siendo del responsable.

---

<sup>1</sup> El término "responsable" identifica a un individuo o una entidad que tiene responsabilidad aprobada de la dirección por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos. El término "responsable" no implica que la persona tenga realmente los derechos de propiedad de los activos.

En los sistemas complejos de información puede ser útil asignar grupos de activos que actúan juntos para suministrar una función particular como "servicios". En este caso, el responsable del servicio es responsable de la entrega de éste, incluyendo el funcionamiento de los activos que lo proporcionan.

#### **2.2.4.1.3 USO ACEPTABLE DE LOS ACTIVOS**

##### **Control**

Se deberían identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información.

##### **Guía de implementación**

Todos los empleados, contratistas y usuarios por tercera parte deberían seguir las reglas para el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de información, incluyendo:

- a) Reglas para el uso del correo electrónico y de Internet.
- b) Directrices para el uso de los dispositivos móviles, especialmente para su utilización fuera de las instalaciones de la organización.

El director correspondiente debería suministrar las reglas o directrices específicas. Los empleados, contratistas y usuarios de tercera parte que utilizan o tienen acceso a los activos de la organización deberían estar conscientes de los límites que existen para el uso de la información y de los activos de la organización asociados con los servicios de procesamiento de información, así como de los recursos. Ellos deberían ser responsables del uso que hagan de los recursos de procesamiento de información y de cualquier uso efectuado bajo su responsabilidad.

## **2.2.4.2 CLASIFICACIÓN DE LA INFORMACIÓN**

Asegurar que la información recibe el nivel de protección adecuado.

La información se debería clasificar para indicar la necesidad, las prioridades y el grado esperado de protección al manejar la información.

La información tiene diferentes grados de sensibilidad e importancia. Algunos elementos pueden requerir un grado adicional de protección o manejo especial. Se recomienda utilizar un esquema de clasificación de la información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas especiales de manejo.

### **2.2.4.2.1 DIRECTRICES DE CLASIFICACIÓN**

#### **Control**

La información se debería clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización.

#### **Guía de implementación**

Las clasificaciones y los controles de protección asociados para la información deberían considerar las necesidades del negocio respecto a compartir o restringir la información, al igual que los impactos del negocio asociados con tales necesidades.

Las directrices de clasificación deberían incluir convenciones para la clasificación inicial y la reclasificación con el paso del tiempo, de acuerdo con alguna política predeterminada de control del acceso.

Debería ser responsabilidad del responsable del activo definir la clasificación del activo, revisarlo periódicamente y asegurarse de que se mantiene actualizado y en el nivel adecuado.

Es conveniente considerar la cantidad de categorías de clasificación y los beneficios a obtener con su utilización. Los esquemas demasiado complejos pueden volverse engorrosos y de uso costoso o no ser prácticos. Se debería tener cuidado al interpretar las etiquetas de clasificación en los documentos de otras organizaciones, las cuales pueden tener diferentes definiciones para etiquetas iguales o similares.

### **Información adicional**

El nivel de protección se puede evaluar analizando la confidencialidad, la integridad y la disponibilidad como también otros requisitos para la información en consideración.

Con frecuencia, la información deja de ser sensible o importante después de un periodo de tiempo dado, por ejemplo, cuando la información se hace pública. Se deberían considerar estos aspectos puesto que la superclasificación puede originar la implementación de controles innecesarios que llevan a un costo adicional.

La consideración de documentos con requisitos de la seguridad similares cuando se asignan los niveles de clasificación puede ser útil para simplificar la labor de clasificación.

En términos generales, la clasificación que se da a la información es una manera corta de determinar la forma en que se debe manejar y proteger esta información.

## **2.2.4.2.2 ETIQUETADO Y MANEJO DE LA INFORMACIÓN**

### **Control**

Se debería desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización.

### **Guía de implementación**

Es necesario que los procedimientos para el etiquetado de la información comprendan los activos de información en formatos físico y electrónico.

Las salidas de los sistemas que contienen información que se clasifica como sensible o crítica deberían portar una etiqueta de clasificación adecuada (en la salida). Los elementos a considerar incluyen informes impresos, presentaciones en pantalla, medios grabados (por ejemplo, cintas, discos, discos compactos), mensajes electrónicos y transferencias de archivos.

Para cada nivel de clasificación es recomendable definir los procedimientos de manejo, incluyendo procesamiento, almacenamiento, transmisión, desclasificación y destrucción seguros. Ello debería incluir los procedimientos para la cadena de custodia y el registro de cualquier evento importante de la seguridad.

Los acuerdos con otras organizaciones que incluyen compartir información deberían incluir procedimientos para identificar la clasificación de dicha información y para interpretar las etiquetas de clasificación de otras organizaciones.

### **Información adicional**

El etiquetado y el manejo seguro de la información clasificada son un requisito clave de los acuerdos para compartir información. Las etiquetas físicas son una forma común de etiquetado.

No obstante, algunos activos de información, tales como los documentos en formato electrónico, no se pueden identificar físicamente y es necesario emplear medios electrónicos de etiquetado. Por ejemplo, el etiquetado de notificación puede aparecer en la pantalla o en la presentación. Cuando el etiquetado no es viable, se pueden aplicar otros medios para designar la clasificación de la información, por ejemplo a través de procedimientos o meta-datos.

## **2.2.5 GESTIÓN DE COMUNICACIONES Y OPERACIONES**

### **2.2.5.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES**

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

Se debería establecer todas las responsabilidades y los procedimientos para la gestión y operación de todos los servicios de procesamiento de información. Esto incluye el desarrollo de procedimientos operativos apropiados.

Cuando sea conveniente, se debería implementar la separación de funciones para reducir el riesgo del uso inadecuado deliberado o negligente del sistema.

#### **2.2.5.1.1 DOCUMENTACIÓN DE LOS PROCEDIMIENTOS DE OPERACIÓN**

##### **Control**

Los procedimientos de operación se deberían documentar, mantener y estar disponibles para todos los usuarios que los necesiten.

##### **Guía de implementación**

Se deberían elaborar procedimientos documentados para las actividades del sistema asociadas con los servicios de comunicaciones y de procesamiento de información, como por ejemplo procedimientos para el encendido y apagado de los computadores, copias de respaldo, mantenimiento de equipos, manejo de los medios, cuarto de equipos y gestión del correo, como también de la seguridad.

Los procedimientos de operación deberían especificar las instrucciones para la ejecución detallada de cada trabajo, incluyendo:

- a) Procesamiento y manejo de información.
- b) Copias de respaldo.
- c) Requisitos de programación, incluyendo las interrelaciones con otros sistemas, hora de comienzo de la tarea inicial y de terminación de la tarea final.
- d) Instrucciones para el manejo de errores y otras condiciones excepcionales que se pueden presentar durante la ejecución del trabajo, incluyendo las restricciones al uso de las utilidades del sistema.
- e) Contactos de soporte en caso de dificultades técnicas u operativas inesperadas.

- f) Instrucciones de manejo de los medios y los informes especiales, como el uso de papelería especial o el manejo de los informes confidenciales incluyendo los procedimientos para la eliminación segura de los informes de tareas fallidas.
- g) Procedimientos para el reinicio y la recuperación del sistema que se han de usar en caso de falla del sistema.
- h) Gestión de los registros de auditoría y de la información de registro del sistema.

Los procedimientos operativos, y los procedimientos documentados para las actividades del sistema, se deberían tratar como documentos formales y sus cambios deberían ser autorizados por la dirección. Cuando sea técnicamente viable, se recomienda gestionar los sistemas de información de forma consistente, utilizando los mismos procedimientos, herramientas y utilidades.

#### **2.2.5.1.2 GESTIÓN DEL CAMBIO**

##### **Control**

Se deberían controlar los cambios en los servicios y los sistemas de procesamiento de información.

##### **Guía de implementación**

Los sistemas operativos y el software de aplicación deberían estar sujetos a un control estricto de la gestión del cambio.

En particular, se deberían considerar los siguientes elementos:

- a) Identificación y registro de los cambios significativos.
- b) Planificación y pruebas de los cambios.
- c) Evaluación de los impactos potenciales de tales cambios, incluyendo los impactos en la seguridad.

- d) Procedimiento de aprobación formal para los cambios propuestos.
- e) Comunicación de los detalles del cambio a todas las personas implicadas.
- f) Procedimientos de emergencia, incluyendo los procedimientos y las responsabilidades de cancelar o recuperarse de cambios fallidos y eventos imprevistos.

Se deberían establecer las responsabilidades y los procedimientos formales de gestión para garantizar el control satisfactorio de todos los cambios en los equipos, el software o los procedimientos. Cuando se realicen los cambios, es conveniente conservar un registro de auditoría que contenga toda la información pertinente.

### **Información adicional**

El control inadecuado de los cambios en los sistemas y los servicios de procesamiento de información es una causa común de falta del sistema o de la seguridad. Los cambios en el entorno operativo, especialmente cuando se transfiere un sistema de la fase de desarrollo a la operativa pueden tener impacto en la confiabilidad de las aplicaciones.

Los cambios en los sistemas operativos sólo se deberían realizar cuando existe una razón válida para el negocio, como por ejemplo un aumento en el riesgo para el sistema. La actualización de los sistemas con las últimas versiones del sistema operativo o de la aplicación no siempre favorece el interés del negocio y ello podría introducir más vulnerabilidades e inestabilidad que la versión vigente. También puede existir la necesidad de formación adicional, costos de licencias, soporte, costos generales de mantenimiento y administración y nuevo hardware, especialmente durante la migración.

### **2.2.5.1.3 DISTRIBUCIÓN DE FUNCIONES**

#### **Control**

Las funciones y las áreas de responsabilidad se deberían distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la organización.



## **Guía de implementación**

La distribución de funciones es un método para reducir el riesgo de uso inadecuado deliberado o accidental del sistema. Se debería tener cuidado de que ninguna persona pueda tener acceso, modificar o utilizar los activos sin autorización o sin ser detectado. La iniciación de un evento se debería separar de su autorización. Es conveniente considerar la posibilidad de complicidad al diseñar los controles.

Las organizaciones pequeñas pueden encontrar difícil de lograr la distribución de funciones, pero el principio se debería aplicar en la medida de lo posible y viable. Cuando haya dificultad para la distribución, se deberían considerar otros controles como monitoreo de actividades, registros de auditoría y supervisión por la dirección. Es importante que la auditoría de la seguridad siga siendo independiente.

### **2.2.5.1.4 SEPARACIÓN DE LAS INSTALACIONES DE DESARROLLO, ENSAYO Y OPERACIÓN**

#### **Control**

Las instalaciones de desarrollo, ensayo y operación deberían estar separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo.

#### **Guía de implementación**

Se debería identificar el grado de separación entre los ambientes operativo, de prueba y de desarrollo que es necesario para prevenir problemas operativos e implementar los controles adecuados.

Se deberían tener presentes los siguientes elementos:

- a) Se recomienda definir y documentar las reglas para la transferencia de software del estado de desarrollo al operativo.
- b) El software de desarrollo y el operativo se deberían ejecutar en diferentes sistemas o procesadores de computación y en diferentes dominios o directorios.

- c) Los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema no deberían ser accesibles desde los sistemas operativos cuando no se requiera.
- d) El ambiente del sistema de prueba debería emular al ambiente del sistema operativo lo más estrechamente posible.
- e) Los usuarios deberían emplear perfiles de usuario diferentes para los sistemas operativos y de prueba y los menús deberían desplegar mensajes de identificación adecuados para reducir el riesgo de error.
- f) Los datos sensibles no se deberían copiar en el entorno del sistema de prueba.

### **Información adicional**

Las actividades de desarrollo y de prueba pueden causar problemas graves, como la modificación indeseada de archivos o del entorno del sistema, o falla del sistema. En este caso, es necesario mantener un entorno conocido y estable en el cual realizar pruebas significativas y evitar el acceso inadecuado de los desarrolladores.

Cuando el personal de desarrollo y de pruebas tiene acceso al sistema operativo y su información, pueden introducir códigos no autorizados y sin probar o alterar los datos operativos. En algunos sistemas, esta capacidad podría ser mal utilizada para cometer fraude o introducir códigos sin probar o maliciosos, lo cual puede crear problemas operativos graves.

Quienes desarrollan y realizan las pruebas imponen una amenaza a la confidencialidad de la información operativa. Las actividades de desarrollo y de prueba pueden causar cambios involuntarios en el software o la información si comparten el mismo entorno de computación.

Por lo tanto, es conveniente separar las instalaciones de desarrollo, de prueba y operativas para reducir el riesgo de cambio accidental o acceso no autorizado al software operativo o a los datos del negocio.

## **2.2.5.2 GESTIÓN DE LA PRESTACIÓN DEL SERVICIO POR TERCERAS PARTES**

Implementar y mantener un grado adecuado de la seguridad de la información y de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceros.

La organización debería verificar la implementación de acuerdos, monitorear el cumplimiento de ellos y gestionar los cambios para asegurar que los servicios que se prestan cumplen los requisitos acordados con los terceros.

### **2.2.5.2.1 PRESTACIÓN DEL SERVICIO**

#### **Control**

Se deberían garantizar que los controles de la seguridad, las definiciones del servicio y los niveles de prestación del servicio incluidos en el acuerdo, sean implementados, mantenidos y operados por el tercero.

#### **Guía de implementación**

La prestación de servicios por terceros debería incluir los acuerdos sobre disposiciones de la seguridad, definiciones del servicio y aspectos de la gestión del mismo. En el caso de contrataciones externas, la organización debería planificar las transiciones necesarias (de información, servicios de procesamiento de información y todo lo demás que se deba transferir) y garantizar que la seguridad se mantiene durante todo el periodo de transición.

Es recomendable que la organización garantice que la tercera parte mantenga una capacidad de servicio suficiente, junto con planes ejecutables diseñados para garantizar la conservación de los niveles de continuidad del servicio acordados, después de desastres o fallas significativas en el servicio.

## **2.2.5.2.2 MONITOREO Y REVISIÓN DE LOS SERVICIOS POR TERCEROS**

### **Control**

Los servicios, reportes y registros suministrados por terceras partes se deberían controlar y revisar con regularidad y las auditorías se deberían llevar a cabo a intervalos regulares.

### **Guía de implementación**

El monitoreo y la revisión de los servicios proporcionados por terceras partes deberían garantizar el cumplimiento de los términos y condiciones de la seguridad de la información, de los acuerdos y que los incidentes y problemas de la seguridad de la información se manejen adecuadamente.

Ello debería implicar una relación y un proceso de gestión del servicio entre la organización y la tercera parte para:

- a) Monitorear los niveles de desempeño del servicio para verificar el cumplimiento de los acuerdos.
- b) Revisar los reportes del servicio elaborados por la tercera parte y acordar reuniones periódicas sobre el progreso, según lo exijan los acuerdos.
- c) Suministrar información sobre los incidentes de la seguridad de la información, y revisión de esta información por parte de la organización y la tercera parte, según lo exijan los acuerdos, directrices y los procedimientos de soporte.
- d) Revisión de los registros y pruebas de auditoría de la tercera parte con respecto a eventos de la seguridad, problemas operativos, fallas, rastreo de fallas e interrupciones relacionadas con el servicio prestado.
- e) Resolver y manejar todos los problemas identificados.

La responsabilidad por la gestión de la relación con la tercera parte se le debería asignar a una persona o a un equipo de gestión del servicio. Además, la organización debería garantizar que la tercera parte asigne responsabilidades para la verificación del cumplimiento y la aplicación de los requisitos de los acuerdos.

Se recomienda poner a disposición suficientes habilidades técnicas y recursos para monitorear el cumplimiento de los requisitos del acuerdo, en particular los requisitos de la seguridad de la información. Cuando se observan deficiencias en la prestación del servicio se deberían tomar las acciones adecuadas.

La organización debería mantener suficiente control global y no perder de vista todos los aspectos de la seguridad para la información sensible o crítica, o de los servicios de procesamiento de información que haya procesado, gestionado o tenido acceso la tercera parte.

La organización debería asegurarse de que conserva visibilidad en las actividades de la seguridad como gestión de cambios, identificación de vulnerabilidades e informe / respuesta de los incidentes de la seguridad de la información a través de un proceso, estructuras y formatos definidos claramente para la presentación de informes.

### **Información adicional**

En caso de contratación externa, es necesario que la organización sepa que la máxima responsabilidad por la información procesada por una parte contratada externamente sigue siendo de la organización.

### **2.2.5.2.3 GESTIÓN DE LOS CAMBIOS EN LOS SERVICIOS POR TERCERAS PARTES**

#### **Control**

Los cambios en la prestación de los servicios, incluyendo mantenimiento y mejora de las políticas existentes de la seguridad de la información, en los procedimientos y los controles se deberían gestionar teniendo en cuenta la importancia de los sistemas y procesos del negocio involucrados, así como la reevaluación de los riesgos.

#### **Guía de implementación**

Es necesario que el proceso de gestión de los cambios en el servicio prestado por la tercera parte tome en consideración:

- a) Los cambios hechos por la organización para implementar:
  - a. Mejoras en los servicios actuales ofrecidos.
  - b. Desarrollo de todos los sistemas o aplicaciones nuevas.
  - c. Modificaciones o actualizaciones de las políticas y procedimientos de la organización.
  - d. Controles nuevos para resolver los incidentes de la seguridad de la información y para mejorar la seguridad.
  
- b) Cambios en los servicios por la tercera parte para implementar:
  - a. Cambios y mejoras en las redes.
  - b. Uso de nuevas tecnologías.
  - c. Adopción de productos nuevos o versiones / divulgaciones más recientes.
  - d. Nuevas herramientas y entornos de desarrollo.
  - e. Cambios en la ubicación física de las instalaciones de los servicios.
  - f. Cambio de proveedores.

### **2.2.5.3 PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA**

Minimizar el riesgo de fallas en los sistemas.

Se requieren una previa planificación y preparación para garantizar la disponibilidad de la capacidad y los recursos adecuados para entregar el desempeño requerido del sistema.

Es necesario hacer proyecciones de la capacidad futura para reducir el riesgo de sobrecarga del sistema.

Los requisitos operativos de los sistemas nuevos se deberían establecer, documentar y probar antes de su aceptación y uso.

### **2.2.5.3.1 GESTIÓN DE LA CAPACIDAD**

#### **Control**

Se debería hacer seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema.

#### **Guía de implementación**

Para cada actividad nueva y existente es conveniente identificar los requisitos de la capacidad.

Se recomienda monitorear y adaptar el sistema para garantizar y, cuando sea necesario, mejorar la capacidad y la eficacia de los sistemas. Se deberían establecer controles de indagación para indicar los problemas en el momento oportuno. En las proyecciones de los requisitos de capacidad futura se deberían considerar los negocios nuevos y los requisitos del sistema, así como las tendencias actuales y proyectadas en la capacidad de procesamiento de información de la organización.

Es necesario poner atención a los recursos cuya adquisición toma mucho tiempo o requiere costos elevados, por lo tanto, los directores deberían monitorear la utilización de los recursos claves del sistema. También deberían identificar las tendencias del uso, particularmente en relación con las aplicaciones del negocio o las herramientas del sistema de información para la gestión.

Es conveniente que los directores utilicen esta información para identificar y evitar posibles cuellos de botella así como la dependencia de personal clave, los cuales pueden presentar una amenaza para los servicios o la seguridad del sistema, y para planificar la acción adecuada.

### **2.2.5.3.2 ACEPTACIÓN DEL SISTEMA**

#### **Control**

Se deberían establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación.

#### **Guía de implementación**

Los directores deberían garantizar que los requisitos y los criterios para la aceptación de sistemas nuevos están definidos, acordados, documentados y probados claramente. Los sistemas de información nuevos, las actualizaciones y las nuevas versiones únicamente deberían migrar a producción después de obtener la aceptación formal. Se deberían considerar los siguientes elementos antes de la aceptación formal:

- a) Requisitos de desempeño y capacidad de los computadores.
- b) Procedimientos de reinicio y de recuperación por errores, y planes de contingencia.
- c) Preparación y prueba de procedimientos operativos de rutina para las normas definidas.
- d) Establecimiento del conjunto de controles de la seguridad acordados.
- e) Procedimientos manuales eficaces.
- f) Disposiciones para la continuidad del negocio.
- g) Evidencia de que la instalación del sistema nuevo no afectará adversamente a los sistemas existentes, particularmente en los momentos pico de procesamiento, como al final de mes.
- h) Evidencia de que se ha tenido en cuenta el efecto del sistema nuevo en toda la seguridad de la organización.



- i) Formación en el funcionamiento o utilización de los sistemas nuevos.
- j) Facilidad de uso, en la medida en que afecte el desempeño del usuario y evite el error humano.

Para nuevos desarrollos importantes se debería consultar a los usuarios y a la función de operaciones en todas las fases del proceso de desarrollo para garantizar la eficiencia operativa del diseño del sistema propuesto. Es conveniente llevar a cabo pruebas adecuadas para confirmar el cumplimiento pleno de todos los criterios de aceptación.

### **Información adicional**

La aceptación puede incluir un proceso formal de certificación y acreditación para verificar que el tratamiento que se ha dado a los requisitos de la seguridad es el adecuado.

#### **2.2.5.4 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS Y MÓVILES**

Proteger la integridad del software y de la información.

Se requieren precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no autorizados.

El software y los servicios de procesamiento de información son vulnerables a la introducción de códigos maliciosos tales como virus de computador, gusanos en la red, caballos troyanos y bombas lógicas. Los usuarios deberían ser conscientes de los peligros de los códigos maliciosos. Los directores deberían, cuando sea apropiado, introducir controles para evitar, detectar y retirar los códigos maliciosos y controlar los códigos móviles.

#### **2.2.5.4.1 CONTROLES CONTRA CÓDIGOS MALICIOSOS**

##### **Control**

Se deberían implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como procedimientos apropiados de concienciación de los usuarios.

##### **Guía de implementación**

La protección contra códigos maliciosos se debería basar en software de detección y reparación de códigos maliciosos, conciencia sobre seguridad, acceso apropiado al sistema y controles en la gestión de cambios. Se recomienda considerar las siguientes directrices:

- a) Establecer una política formal que prohíba el uso de software no autorizado.
- b) Establecer una política formal para la protección contra los riesgos asociados con la obtención de archivos y software, bien sea desde o a través de redes externas o cualquier otro medio, indicando las medidas de protección que se deberían tomar.
- c) Llevar a cabo revisiones regulares del software y del contenido de datos de los sistemas que dan soporte a los procesos críticos del negocio. se debería investigar formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
- d) Instalación y actualización regular del software de detección y reparación de códigos maliciosos para explorar los computadores y los medios, como control preventivo o de forma rutinaria, las verificaciones realizadas deberían incluir:
  - a. Verificación de la presencia de códigos maliciosos en todos los archivos en medios ópticos o electrónicos y archivos recibidos en las redes antes de su uso.

- b. Verificación de la presencia de códigos maliciosos en los adjuntos y las descargas del correo electrónico antes del uso. esta verificación se debería efectuar en diferentes lugares, por ejemplo en los servidores de correo electrónico, los computadores de escritorio y cuando ingresan a la red de la organización.
- c. Verificación de las páginas web para comprobar la presencia de códigos maliciosos.
- e) Definir responsabilidades y procedimientos de gestión para tratar la protección contra códigos maliciosos en los sistemas, la formación sobre su uso, el reporte y la recuperación debido a ataques de códigos maliciosos.
- f) Preparación de planes adecuados para la continuidad del negocio con el fin de recuperarse de los ataques de códigos maliciosos, incluyendo todos los datos y el soporte de software necesario y las disposiciones para la recuperación.
- g) Implementación de procedimientos para recolectar información con regularidad, como la suscripción a sitios web de verificación y/o listados de correo que suministren información sobre los códigos maliciosos nuevos.
- h) Implementación de procedimientos para verificar la información relacionada con códigos maliciosos y garantizar que los boletines de advertencia sean exactos e informativos. los directores deberían garantizar que se utilizan fuentes calificadas, por ejemplo diarios reconocidos, sitios confiables de internet o proveedores de software de protección contra códigos maliciosos para diferenciar entre falsas alarmas y códigos maliciosos reales. todos los usuarios deberían conocer el problema de las falsas alarmas y qué hacer al recibirlas.

### **Información adicional**

El empleo de dos o más productos de software, de diferentes proveedores, que protejan contra códigos maliciosos a través de todo el entorno de procesamiento de información puede mejorar la eficacia de la protección contra códigos maliciosos.

El software de protección contra códigos maliciosos se puede instalar para que suministre actualizaciones automáticas de los archivos de definición y de los motores de exploración para garantizar que la protección esté al día. Además, este software se puede instalar en cada escritorio para realizar verificaciones automáticas.

Se debe tener cuidado para la protección contra la introducción de códigos maliciosos durante los procedimientos de mantenimiento y de emergencia, ya que se pueden eludir los controles normales de protección contra códigos maliciosos.

#### **2.2.5.4.2 CONTROLES CONTRA CÓDIGOS MÓVILES**

##### **Control**

Cuando se autoriza la utilización de códigos móviles, la configuración debería asegurar que dichos códigos operan de acuerdo con la política de la seguridad claramente definida, y se debería evitar la ejecución de los códigos móviles no autorizados.

##### **Guía de implementación**

Se recomienda tener en cuenta las siguientes consideraciones para la protección contra códigos móviles que ejecutan acciones no autorizadas:

- a) Ejecución de los códigos móviles en un entorno con aislamiento lógico.
- b) Bloqueo de cualquier uso de códigos móviles.
- c) Bloqueo de la recepción de códigos móviles.
- d) Activación de medidas técnicas, según estén disponibles, en un sistema específico para garantizar la gestión del código móvil.
- e) Control de recursos disponibles para el acceso a códigos móviles.
- f) Controles criptográficos para autenticar de forma única el código móvil.

## **Información adicional**

El código móvil es un código de software que se transfiere de un computador a otro y luego se ejecuta automáticamente y lleva a cabo una función específica con poca o ninguna interacción del usuario. El código móvil se asocia con una variedad de servicios intermedios (middleware).

Además, para garantizar que el código móvil no contiene código malicioso, el control del código móvil es esencial para evitar el uso no autorizado o la interrupción del sistema, la red o los recursos de aplicación y otras brechas de la seguridad de la información.

### **2.2.5.5 RESPALDO**

Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.

Se deberían establecer procedimientos de rutina para implementar la política y la estrategia de respaldo acordada para hacer copias de la seguridad de los datos y probar sus tiempos de restauración.

#### **2.2.5.5.1 RESPALDO DE LA INFORMACIÓN**

##### **Control**

Se deberían hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.

Es conveniente disponer de servicios de respaldo adecuados para garantizar que la información y el software esenciales se recuperan después de un desastre o una falla de los medios.

Se recomienda considerar los siguientes elementos para el respaldo de la información:

- a) Es recomendable definir el nivel necesario para la información de respaldo.

- b) Se deberían hacer registros exactos y completos de las copias de respaldo y generar procedimientos documentados de restauración.
- c) La extensión (por ejemplo respaldo completo o diferencial) y la frecuencia de los respaldos debería reflejar los requisitos del negocio de la organización, los requisitos de la seguridad de la información involucrada y la importancia de la operación continua de la organización.
- d) Los respaldos se deberían almacenar en un sitio lejano, a una distancia suficiente para escapar a cualquier daño debido a desastres en la sede principal.
- e) A la información de respaldo se le debería dar un grado apropiado de protección física y ambiental consistente con las normas aplicadas en la sede principal. los controles aplicados a los medios en la sede principal se deberían extender para cubrir el sitio en donde está el respaldo.
- f) Es conveniente probar con regularidad los medios de respaldo para garantizar que sean confiables para uso en emergencias, cuando sea necesario.
- g) Los procedimientos de restauración se deberían verificar y probar con regularidad para garantizar su eficacia y que se pueden completar dentro del tiempo designado en los procedimientos operativos para la recuperación.
- h) En situaciones en donde es importante la confidencialidad, los respaldos se deberían proteger por medio de encriptación.

Las disposiciones de respaldo para los sistemas individuales se deberían someter a prueba con regularidad para garantizar que cumplen los requisitos de los planes para la continuidad del negocio. Para sistemas críticos, las disposiciones de respaldo deberían comprender toda la información de los sistemas, las aplicaciones y los datos necesarios para recuperar todo el sistema en caso de desastre.

Es necesario determinar el período de retención de la información esencial para el negocio, así como cualquier requisito para retener permanentemente las copias de archivo.

## **Información adicional**

Las disposiciones de respaldo se pueden automatizar para facilitar el respaldo y el proceso de restauración. Las soluciones automatizadas deberían probarse suficientemente antes de la implementación y a intervalos regulares.

### **2.2.5.6 GESTIÓN DE LA SEGURIDAD DE LAS REDES**

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

La gestión segura de las redes, las cuales pueden sobrepasar las fronteras de la organización, exige la consideración cuidadosa del flujo de datos, las implicaciones legales, el monitoreo y la protección.

También pueden ser necesarios los controles adicionales para proteger la información sensible que pasa por las redes públicas.

#### **2.2.5.6.1 CONTROLES DE LAS REDES**

##### **Control**

Las redes se deberían mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.

##### **Guía de implementación**

Los directores de la red deberían implementar controles que garanticen la seguridad de la información sobre las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, es conveniente tener en cuenta los siguientes elementos:

- a) La responsabilidad operativa por las redes debería estar separada de las operaciones de computador, según sea apropiado.

- b) Es necesario establecer las responsabilidades y los procedimientos para la gestión de equipos remotos, incluyendo los equipos en áreas de usuarios.
- c) Es conveniente establecer controles especiales para salvaguardar la confidencialidad y la integridad de los datos que pasan por redes públicas o redes inalámbricas y para proteger los sistemas y las aplicaciones conectadas. también se pueden requerir controles especiales para mantener la disponibilidad de los servicios de la red y los computadores conectados.
- d) Se deberían aplicar el registro y el monitoreo adecuados para permitir el registro de acciones de la seguridad pertinentes.
- e) Se recomienda coordinar estrechamente las actividades de gestión tanto para optimizar el servicio para la organización como para garantizar que los controles se aplican consistentemente en toda la infraestructura del procesamiento de información.

#### **2.2.5.6.2 SEGURIDAD DE LOS SERVICIOS DE LA RED**

##### **Control**

En cualquier acuerdo sobre los servicios de la red se deberían identificar e incluir las características de la seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios se prestan en la organización o se contratan externamente.

##### **Guía de implementación**

La capacidad del proveedor del servicio de red para gestionar los servicios acordados de forma segura se debería determinar y monitorear regularmente, y se debería acordar el derecho a auditoría.

Se deberían identificar las disposiciones de la seguridad necesarias para servicios particulares, tales como las características de la seguridad, los niveles de servicio y los requisitos de gestión.

La organización debería garantizar que los proveedores de servicios de red implementan estas medidas.



## **Información adicional**

Los servicios de red incluyen la provisión de conexiones, servicios de red privada y redes con valor agregado, así como soluciones de la seguridad de red administrada, como por ejemplo cortafuegos (Firewalls) y sistemas de detección de intrusión. Estos servicios pueden ir desde simples anchos de banda no administrados hasta ofertas complejas de valor agregado.

Las características de los servicios de red podrían ser:

- a) Tecnología aplicada para la seguridad de los servicios de red, como la autenticación, la encriptación y los controles de conexión de red.
- b) Parámetros técnicos requeridos para la conexión segura a los servicios de red según las reglas de la seguridad y conexión de red.
- c) Procedimientos para la utilización de los servicios de red para restringir el acceso a los servicios de red o a las aplicaciones, cuando sea necesario.

### **2.2.5.7 MANEJO DE LOS MEDIOS**

Evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del negocio.

Estos medios se deberían controlar y proteger de forma física.

Se deberían establecer procedimientos operativos adecuados para proteger documentos, medios de computador (por ejemplo cintas, discos), datos de entrada/salida y documentación del sistema contra divulgación, modificación, remoción y destrucción no autorizadas.

### **2.2.5.7.1 GESTIÓN DE LOS MEDIOS REMOVIBLES**

#### **Control**

Se deberían establecer procedimientos para la gestión de los medios removibles.

#### **Guía de implementación**

Se recomienda tener presentes las siguientes directrices:

- a) Si ya no son necesarios, los contenidos de todos los medios reutilizables que se van a retirar de la organización se deberían hacer irrecuperables.
- b) Cuando sea necesario y práctico, se debería exigir autorización para los medios retirados de la organización y conservar un registro de tales retiros para mantener una prueba de auditoría.
- c) Todos los medios se deberían almacenar en un ambiente seguro y vigilado, según las especificaciones del fabricante.
- d) La información almacenada en los medios que debe estar disponible por más tiempo del de la vida del medio (según las especificaciones del fabricante) también se debería almacenar en otra parte para evitar la pérdida de información debido al deterioro de dichos medios.
- e) Se debería tener en cuenta el registro de los medios removibles para evitar la oportunidad de que se presente pérdida de datos.
- f) Las unidades de medios removibles sólo se deberían habilitar si existen razones del negocio para hacerlo.

Todos los procedimientos y niveles de autorización deberían estar documentados con claridad.

## **Información adicional**

Los medios removibles incluyen cintas, discos, memorias de almacenamiento, unidades de almacenamiento removibles, discos compactos, discos de video digital (DVD) y medios impresos.

### **2.2.5.7.2 ELIMINACIÓN DE LOS MEDIOS**

#### **Control**

Cuando ya no se requieren estos medios, su eliminación se debería hacer de forma segura y sin riesgo, utilizando los procedimientos formales.

#### **Guía de implementación**

Los procedimientos formales para la eliminación segura de los medios deberían minimizar el riesgo de fuga de Información sensible a personas no autorizadas. Los procedimientos para la eliminación segura de los medios que contienen información sensible deberían estar acordes con la sensibilidad de dicha información. Se recomienda tener en cuenta los siguientes elementos:

- a) Los medios que contienen información sensible se deberían almacenar y eliminar de forma segura e inocua, por ejemplo mediante incineración o trituración, o borrar los datos para evitar el uso por parte de otra aplicación en la organización.
- b) Se deberían establecer procedimientos para identificar los elementos que pueden requerir eliminación segura.
- c) Puede ser más fácil disponer de todos los elementos de los medios de almacenamiento que serán recogidos y liberados de forma segura, que tratar de disponer sólo de los elementos sensibles.
- d) Muchas organizaciones ofrecen servicios de recolección y eliminación de papel, equipos y medios. se debe tener cuidado en seleccionar un contratista idóneo con controles y experiencia adecuados.

- e) Cuando sea posible, se debería registrar la eliminación de los elementos sensibles con el objeto de mantener una prueba de auditoría.

Cuando se acumulan medios para su eliminación se debería considerar el efecto de agregación, el cual puede hacer que una gran cantidad de información no sensible se vuelve sensible.

### **Información adicional**

Se podría divulgar información sensible debido a la eliminación descuida del medio.

### **2.2.5.7.3 PROCEDIMIENTOS PARA EL MANEJO DE LA INFORMACIÓN**

#### **Control**

Se deberían establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.

#### **Guía de implementación**

Se deberían elaborar procedimientos para manejar, procesar, almacenar y comunicar la información de acuerdo con su clasificación. Se deberían considerar los siguientes elementos:

- a) Manejo y etiquetado de todos los medios hasta su nivel indicado de clasificación.
- b) Restricciones de acceso para evitar el acceso de personal no autorizado.
- c) Mantenimiento de un registro formal de los receptores autorizados de los datos.
- d) Garantizar que los datos de entrada están completos, que el procesamiento se completa adecuadamente y que se aplica la validación de la salida.
- e) Protección, según su nivel de sensibilidad, de los datos de la memoria temporal que esperan su ejecución.

- f) Almacenamiento de los medios según las especificaciones del fabricante.
- g) Mantenimiento de la distribución de datos en un mínimo.
- h) Rotulado claro de todas las copias de los medios para la autenticación del receptor autorizado.
- i) Revisión de las listas de distribución y las listas de receptores autorizados a intervalos regulares.

### **Información adicional**

Estos procedimientos se aplican a la información en documentos, sistemas de computación, redes, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, prestaciones / servicios postales, uso de máquinas de fax y a todos los elementos sensibles, como cheques en blanco y facturas.

#### **2.2.5.7.4 SEGURIDAD DE LA DOCUMENTACIÓN DEL SISTEMA**

##### **Control**

La documentación del sistema debería estar protegida contra el acceso no autorizado.

##### **Guía de implementación**

Para asegurar la documentación del sistema, se deberían tener en cuenta los siguientes elementos:

- a) La documentación del sistema se debería almacenar con seguridad.
- b) La lista de acceso a la documentación del sistema se debería mantener mínima y debería estar autorizada por el responsable de la aplicación.
- c) La documentación del sistema en la red pública o que se suministra a través de una red pública, debería tener protección adecuada.

## **Información adicional**

La documentación del sistema puede contener variada información sensible, como descripciones de procesos de aplicación, procedimientos, estructuras de datos y procesos de autorización.

### **2.2.5.8 INTERCAMBIO DE LA INFORMACIÓN**

Mantener la seguridad de la información y del software que se intercambian dentro de la organización y con cualquier entidad externa.

Los intercambios de información y de software entre las organizaciones se deberían basar en una política formal de intercambio, ejecutar según los acuerdos de intercambio y cumplir la legislación correspondiente.

Se deberían establecer procedimientos y normas para proteger la información y los medios físicos que contienen información en tránsito.

#### **2.2.5.8.1 POLÍTICAS Y PROCEDIMIENTOS PARA EL INTERCAMBIO DE INFORMACIÓN**

##### **Control**

Se deberían establecer políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de servicios de comunicación.

##### **Guía de implementación**

Los procedimientos y controles a seguir cuando se utilizan servicios de comunicación electrónica para el intercambio de información deberían considerar los siguientes elementos:

- a) Procedimientos diseñados para proteger la información intercambiada contra interceptación, copiado, modificación, enrutamiento inadecuado y destrucción.

- b) Procedimientos para detección y protección contra códigos maliciosos que se pueden transmitir con el uso de comunicaciones electrónicas.
- c) Procedimientos para proteger la información electrónica sensible comunicada que está en forma de adjunto.
- d) Políticas o directrices que enfatizan el uso aceptable de los servicios de comunicación electrónica.
- e) Procedimientos para el uso de comunicaciones inalámbricas, pensando en los riesgos particulares involucrados.
- f) Responsabilidades de empleados, contratistas y cualquier otro usuario de no comprometer a la organización, por ejemplo a través de difamación, acoso, suplantación de identidad, envío de cartas de cadena, adquisición no autorizada, etc.
- g) Uso de técnicas criptográficas, por ejemplo para proteger la confidencialidad, la integridad y la autenticidad de la información.
- h) Directrices de retención y eliminación para toda la correspondencia, incluyendo mensajes, según la legislación y los reglamentos locales y nacionales correspondientes.
- i) No dejar información sensible o crítica en los dispositivos de impresión como copadoras, impresoras y máquinas de fax ya que se puede permitir el acceso de personal no autorizado.
- j) Controles y restricciones asociados con el envío de servicios de comunicación, como el envío automático de correo electrónico a direcciones de correo externas.
- k) Recordar al personal que deberían tomar precauciones adecuadas como, por ejemplo, no revelar información sensible para evitar que, cuando se hace una llamada telefónica, sea interceptada o escuchada por:
  - a. Personas en la cercanía inmediata, particularmente cuando se utilizan teléfonos móviles.

- b. Intercepciones telefónicas u otras formas de escuchar no autorizadas mediante el acceso físico al auricular o a la línea telefónica, o usando receptores de exploración.
  - c. Personal al lado del receptor.
- l) No dejar mensajes que contengan información sensible en el contestador automático ya que pueden volver a ser escuchados por personas no autorizadas, almacenados en sistemas comunales o almacenados incorrectamente como resultado de una marcación errónea.
- m) Recordar el personal sobre los problemas de usar máquinas de fax, principalmente:
  - a. Creación de acceso no autorizado en los almacenes de mensajes para recuperar los mensajes.
  - b. Programación deliberada o accidental de máquinas para enviar mensajes a números específicos.
  - c. Envío de documentos y mensajes al número equivocado, bien sea por marcación errónea o por usar el número almacenado erróneamente.
- n) Recordar al personal no registrar datos demográficos, como direcciones de correo electrónico u otra información personal, en ningún software para evitar su recolección para uso no autorizado.
- o) Recordar al personal que las máquinas modernas de fax y las fotocopiadoras tienen páginas de almacenamiento y cache, en caso de falla en el papel o en la transmisión, que se pueden imprimir una vez se ha solucionado la falla.

Además, se debería recordar al personal que no debería tener conversaciones confidenciales en lugares públicos ni oficinas abiertas, como tampoco en lugares de reunión sin paredes a prueba de sonido:

Los servicios de intercambio de información deberían cumplir todos los requisitos legales pertinentes.



## **Información adicional**

El intercambio de información se puede producir a través de la utilización de diferentes tipos de servicios de comunicación, incluyendo correo electrónico, voz, fax y video.

El intercambio de software se puede dar a través de diferentes medios, incluyendo descargas desde internet y adquiridas de vendedores de productos de mostrador.

El negocio debería considerar las implicaciones legales y de la seguridad asociada con el intercambio electrónico de datos, el comercio electrónico y las comunicaciones electrónicas, así como los requisitos para los controles.

La información podría verse amenazada debido a la falta de conciencia, de políticas o procedimientos sobre el uso de los servicios de intercambio de información, por ejemplo por la escucha en un teléfono móvil en un lugar público, la dirección incorrecta de un mensaje de correo electrónico, la escucha de los contestadores automáticos, el acceso no autorizado a sistemas de correo de voz de marcación o el envío accidental de facsímiles al equipo errado de fax.

Las operaciones del negocio podrían ser afectadas y la información podría ser comprometida si los servicios de comunicación fallan, se sobrecargan o interrumpen. La información se vería comprometida por el acceso de usuarios no autorizados.

### **2.2.5.8.2 ACUERDOS PARA EL INTERCAMBIO**

#### **Control**

Se deberían establecer acuerdos para el intercambio de la información y del software entre la organización y las partes externas.

## Guía de implementación

En los acuerdos de intercambio se deberían tomar en consideración las siguientes condiciones de la seguridad:

- a) Responsabilidades de la dirección para controlar y notificar la transmisión, el despacho y la recepción.
- b) Procedimientos para notificar a quien envía la transmisión, el despacho y la recepción.
- c) Procedimientos para garantizar la trazabilidad y el no – repudio.
- d) Normas técnicas mínimas para el empaquetado y la transmisión.
- e) Acuerdos de fideicomiso.
- f) Normas para identificar los servicios de mensajería.
- g) Responsabilidades y deberes en caso de incidentes de la seguridad de la información, como la pérdida de datos.
- h) Uso de sistemas acordados de etiquetado de la información sensible o crítica, garantizando que el significado de las etiquetas se entienda inmediatamente y que la información está protegida adecuadamente.
- i) Propiedad y responsabilidades para la protección de datos, derechos de copia, conformidad de las licencias de software y consideraciones similares.
- j) Normas técnicas para registrar y leer la información y el software.
- k) Todos los controles especiales que se puedan requerir para proteger los elementos sensibles tales como las claves criptográficas.

Se deberían establecer y conservar políticas, procedimientos y normas para proteger la información y los medios físicos en tránsito y ellos se deberían referenciar en dichos acuerdos de intercambio.

El contenido sobre seguridad de cualquier acuerdo debería reflejar la sensibilidad de la información del negocio involucrada.

### **Información adicional**

Los acuerdos pueden ser electrónicos o manuales y pueden tomar la forma de contratos formales o condiciones de empleo. Para la información sensible, los mecanismos específicos utilizados para el intercambio de dicha información deberían ser consistentes para todas las organizaciones y todos los tipos de acuerdos.

### **2.2.5.8.3 MEDIOS FÍSICOS EN TRÁNSITO**

#### **Control**

Los medios que contienen información se deberían proteger contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de los límites físicos de la organización.

#### **Guía de implementación**

Se recomienda tener en cuenta las siguientes directrices para la protección de los medios que se transportan entre los lugares:

- a) Se recomienda utilizar transporte confiable o servicios de mensajería.
- b) Se debería acordar con la dirección una lista de servicios de mensajería.
- c) Se deberían desarrollar procedimientos para verificar la identificación de los servicios de mensajería.
- d) El embalaje debería ser suficiente para proteger el contenido contra cualquier daño físico potencial que se pueda producir durante el transporte, y estar acorde con las especificaciones del fabricante (por ejemplo para el software), por ejemplo protección contra todos los factores ambientales que puedan reducir la eficacia de la restauración de los medios tal como la exposición al calor, la humedad o los campos electromagnéticos.

- e) Cuando sea necesario, se deberían adoptar controles para proteger la información sensible contra divulgación o modificación no autorizada. algunos ejemplos incluyen.
  - a. Uso de contenedores cerrados con llave.
  - b. Entrega personal.
  - c. Embalajes con sello de la seguridad (que revelan cualquier intento de acceso).
  - d. En casos excepcionales, división de la remesa en más de una entrega y despacho por rutas diferentes.

### **Información adicional**

La información puede ser vulnerable al acceso no autorizado, al uso inadecuado o a la corrupción durante el transporte físico, es el caso de los envíos de medios a través de servicios postales o de mensajería.

#### **2.2.5.8.4 MENSAJERÍA ELECTRÓNICA**

##### **Control**

La Información contenida en la mensajería electrónica debería tener la protección adecuada.

##### **Guía de implementación**

Las consideraciones de la seguridad para la mensajería electrónica deberían incluir las siguientes:

- a) Proteger los mensajes contra acceso no autorizado, modificación o negación de los servicios.
- b) Garantizar que la dirección y el transporte del mensaje son correctos.

- c) Confiabilidad general y disponibilidad del servicio.
- d) Consideraciones legales como, por ejemplo, los requisitos para las firmas electrónicas.
- e) Obtención de aprobación antes de utilizar servicios públicos externos como la mensajería instantánea o el compartir archivos.
- f) Niveles más sólidos de autenticación que controlen el acceso desde redes accesibles al público.

### **Información adicional**

La mensajería electrónica como, por ejemplo, el correo electrónico, el intercambio de datos electrónicos (EDI) y la mensajería instantánea tienen una función cada vez más creciente en las comunicaciones de los negocios. La mensajería electrónica tiene riesgos diferentes que las comunicaciones en papel.

### **2.2.5.8.5 SISTEMAS DE INFORMACIÓN DEL NEGOCIO**

#### **Control**

Se deberían establecer, desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información del negocio.

#### **Guía de implementación**

Las consideraciones de las implicaciones que tiene la interconexión de tales servicios para la seguridad y para el negocio deberían incluir:

- a) Vulnerabilidades conocidas en los sistemas administrativos y contables en donde la información es compartida entre diferentes partes de la organización.

- b) Vulnerabilidades de la información en los sistemas de comunicación del negocio, por ejemplo la grabación de llamadas telefónicas o llamadas de conferencias, confidencialidad de las llamadas, almacenamiento de faxes, apertura de correo, distribución del correo.
- c) Política y controles adecuados para gestionar la forma en que se comparte la información.
- d) Categorías excluyentes de información sensible para la organización y documentos clasificados, si los sistemas no brindan un nivel adecuado de protección.
- e) Restricción del acceso a la información diaria relacionada con individuos seleccionados, por ejemplo el personal que trabaja en proyectos sensibles.
- f) Categorías de personal, contratistas o socios del negocio a quienes se permite usar el sistema y los sitios desde los cuales pueden tener acceso.
- g) Restricción de los servicios seleccionados para categorías de usuarios específicos.
- h) Identificación del estado de los usuarios, por ejemplo empleados de la organización o contratistas, en los directorios para el beneficio de otros usuarios.
- i) Retención y copias de respaldo de la información contenida en el sistema.
- j) Requisitos y disposiciones para los recursos de emergencia.

### **Información adicional**

Los sistemas de información de las oficinas son oportunidades para diseminar y compartir más rápido la información del negocio utilizando una combinación de: documentos, computadores, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios / prestaciones postales y máquinas de fax.

## **2.2.5.9 SERVICIOS DE COMERCIO ELECTRÓNICO**

Garantizar la seguridad de los servicios de comercio electrónico y su utilización segura.

Es necesario considerar las implicaciones de la seguridad asociadas al uso de servicios de comercio electrónico, incluyendo las transacciones en línea y los requisitos para los controles.

También se deberían considerar la integridad y disponibilidad de la información publicada electrónicamente a través de sistemas disponibles al público.

### **2.2.5.9.1 COMERCIO ELECTRÓNICO**

#### **Control**

La información involucrada en el comercio electrónico que se transmite por las redes públicas debería estar protegida contra actividades fraudulentas, disputas por contratos y divulgación o modificación no autorizada.

#### **Guía de implementación**

Las consideraciones de la seguridad para el comercio electrónico deberían incluir las siguientes:

- a) El nivel de confianza que exige cada parte en la identidad declarada de las otras partes, por ejemplo por medio de autenticación.
- b) Los procesos de autorización asociados con la persona que puede establecer precios, emitir o firmar documentos comerciales clave.
- c) La garantía de que los socios comerciales están totalmente informados sobre sus autorizaciones.
- d) La determinación y el cumplimiento de los requisitos de confidencialidad, integridad, prueba de despacho y recibo de documentos clave, y el no repudio de contratos, por ejemplos los asociados a los procesos de licitación y contratos.

- e) El nivel de confianza exigido en la integridad de las listas publicadas de precios.
- f) La confidencialidad de datos o información sensible.
- g) La confidencialidad e integridad de las transacciones de orden de compra, información sobre pagos, detalles de las direcciones de entrega y confirmación de recibo.
- h) El grado adecuado de verificación para comprobar la información sobre pagos suministrada por un cliente.
- i) La selección del mejor convenio sobre la forma de pago más apropiada para evitar el fraude.
- j) El nivel de protección exigido para mantener la confidencialidad e integridad de la información de orden de compra.
- k) La evitación de la pérdida o duplicación de la información sobre transacciones.
- l) La responsabilidad asociada con transacciones fraudulentas.
- m) Los requisitos de las pólizas de seguros.

Muchas de las consideraciones anteriores se pueden abordar mediante la aplicación de controles criptográficos, teniendo en cuenta el cumplimiento de los requisitos legales.

Los acuerdos de comercio electrónico entre socios comerciales deberían estar sustentados por un acuerdo documentado que comprometa a ambas partes con los términos acordados, incluyendo detalles sobre la autorización. Pueden ser necesarios otros acuerdos con los proveedores del servicio de información y de la red con valor agregado.

Los sistemas de comercio público deberían publicar sus términos del negocio a los clientes.



También se debería considerar la resistencia al ataque del servidor central (host) utilizado para el comercio electrónico y las implicaciones de la seguridad de cualquier interconexión de red necesaria para la implementación de los servicios de comercio electrónico.

### **Información adicional**

El comercio electrónico es vulnerable a una variedad de amenazas en la red que pueden ocasionar actividad fraudulenta, disputas por contratos y divulgación o modificación de información.

El comercio electrónico puede utilizar métodos de autenticación seguros, por ejemplo el uso de criptografía clave pública y firmas digitales para reducir el riesgo. También se pueden utilizar terceras partes confiables, cuando se necesitan tales servicios.

### **2.2.5.9.2 TRANSACCIONES EN LÍNEA**

#### **Control**

La información involucrada en las transacciones en línea debería estar protegida para evitar transmisión incompleta, enrutamiento inadecuado, alteración, divulgación, duplicación o repetición no autorizada del mensaje.

#### **Guía de implementación**

Las consideraciones de la seguridad para las transacciones en línea deberían incluir las siguientes:

- a) Uso de firmas electrónicas por cada una de las partes implicadas en la transacción.
- b) Todos los aspectos de la transacción, es decir, garantizar que:
  - a. Las credenciales de usuario de todas las partes válidas y se han verificado.
  - b. La transacción sigue siendo confidencial.

- c. Se conserva la privacidad asociada con todas las partes.
- c) Encriptación de la ruta para las comunicaciones entre todas las partes involucradas.
- d) Seguridad de los protocolos utilizados para la comunicación entre todas las partes involucradas.
- e) Garantizar que el almacenamiento de los detalles de la transacción está fuera de cualquier entorno de acceso público, por ejemplo en una plataforma de almacenamiento existente en la intranet de la organización, y que no se retiene ni expone en un medio de almacenamiento accesible directamente desde internet.
- f) Cuando se emplea una autoridad confiable (por ejemplo para propósitos de emitir y mantener firmas digitales y/o certificados digitales) la seguridad se integra e incorpora a través de todo el proceso completo de gestión del certificado/firma.

### **Información adicional**

La extensión de los controles adoptados deberá estar acorde con el nivel de riesgo asociado con cada una de las formas de transacción en línea.

Puede ser necesario que las transacciones cumplan las leyes, las reglas y los reglamentos en la jurisdicción en la cual se genera la transacción, se procesa, se termina y/o almacena.

Existen muchas formas de transacciones que se pueden efectuar en línea, por ejemplo contractuales, financieras, etc.

### **2.2.5.9.3 INFORMACIÓN DISPONIBLE AL PÚBLICO**

#### **Control**

La integridad de la información que se pone a disposición en un sistema de acceso público deberla estar protegida para evitar la modificación no autorizada.

## **Guía de implementación**

El software, los datos y otra información que requiere un nivel alto de integridad que se pone a disposición en sistemas públicos se debería proteger con mecanismos apropiados como firmas digitales. Los sistemas de acceso público se deberían probar frente a debilidades y fallas antes de que la información esté disponible.

Debería existir un proceso formal de aprobación previo a que la información esté disponible al público. Además, todas las entradas suministradas desde el exterior del sistema se deberían verificar y aprobar.

Los sistemas de publicación electrónica, especialmente aquellos que permiten retroalimentación y entrada directa de información, se deberían controlar cuidadosamente de modo que:

- a) La información se obtenga de conformidad con toda la legislación sobre protección de datos.
- b) La entrada de información hacia y procesada por el sistema de publicación se procese completa y exactamente de forma oportuna.
- c) La información sensible estará protegida durante la recolección, el procesamiento y el almacenamiento.
- d) El acceso al sistema de publicación no permite acceso involuntario a redes a las cuales se conecta el sistema.

## **Información adicional**

Puede ser necesario que la información en un sistema disponible al público, por ejemplo la información en un servidor web accesible a través de internet, cumpla las leyes, las reglas y los reglamentos en la jurisdicción en la cual se localiza el sistema, donde tiene lugar el intercambio o donde reside el responsable. La modificación no autorizada de la información pública puede dañar la reputación de la organización de la publicación.

## **2.2.5.10 MONITOREO**

Detectar actividades de procesamiento de la información no autorizadas.

Se deberían monitorear los sistemas y registrar los eventos de la seguridad de la información. Los registros de operador y la actividad de registro de fallas se deberían utilizar para garantizar la identificación de los problemas del sistema de información.

Una organización debería cumplir todos los requisitos legales pertinentes que se aplican a sus actividades de monitoreo y registro.

Debería emplearse el monitoreo del sistema para verificar la eficiencia de los controles adoptados y revisar el cumplimiento de un modelo de política de acceso.

### **2.2.5.10.1 REGISTRO DE AUDITORÍAS**

#### **Control**

Se deberían elaborar y mantener durante un periodo acordado las grabaciones de los registros para auditoría de las actividades de los usuarios, las excepciones y los eventos de la seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso.

#### **Guía de implementación**

Los registros para auditoría deberían incluir, cuando corresponda:

- a) Identificación (ID) de usuario.
- b) Fecha, hora y detalles de los eventos clave, por ejemplo registro de inicio y registro de cierre.
- c) Identidad o ubicación del terminal, si es posible.
- d) Registros de los intentos aceptados y rechazados de acceso al sistema.

- e) Registros de los intentos aceptados y rechazados de acceso a los datos y otros recursos.
- f) Cambios en la configuración del sistema.
- g) Uso de privilegios.
- h) Uso de las utilidades y aplicaciones del sistema.
- i) Archivos a los que se ha tenido acceso y tipo de acceso.
- j) Direcciones y protocolos de red.
- k) Alarmas originadas por el sistema de control del acceso.
- l) Activación y desactivación de los sistemas de protección, como los sistemas antivirus y los sistemas de detección de intrusión.

### **Información adicional**

Los registros para auditoría pueden contener datos personales confidenciales e indiscretos. Se deberían tomar medidas adecuadas para la protección de la privacidad. Cuando sea posible, los administradores del sistema no deberían tener autorización para borrar ni desactivar registros de sus propias actividades.

### **2.2.5.10.2 MONITOREO DE USO DEL SISTEMA**

#### **Control**

Se deberían establecer procedimientos para el monitoreo de uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se deberían revisar con regularidad.

## Guía de implementación

El nivel de monitoreo necesario para servicios individuales se debería determinar mediante una evaluación de riesgos. La organización debería cumplir todos los requisitos legales que se apliquen a sus actividades de monitoreo.

Las áreas que se deberían considerar incluyen:

- a) Acceso autorizado, incluyendo detalles como:
  - a. Identificación de usuario (ID).
  - b. Fecha y hora de eventos clave.
  - c. Tipo de eventos.
  - d. Archivos a los que se ha tenido acceso.
  - e. Programas / utilidades empleados.
- b) Todas las operaciones privilegiadas como:
  - a. Uso de cuentas privilegiadas, por ejemplo supervisor, raíz, administrador.
  - b. Encendido y detención del sistema.
  - c. Acople / desacople del dispositivo de entrada / salida (I/O).
- c) Intentos de acceso no autorizado, tales como:
  - a. Acciones de usuario fallidas o rechazadas.
  - b. Acciones fallidas o rechazadas que implican datos y otros recursos.
  - c. Violaciones de la política de acceso y notificaciones para los cortafuegos (firewalls) y puertas de enlace (gateways).
  - d. Alertas de los sistemas de detección de intrusión de responsable.

- d) Alertas o fallas del sistema como:
  - a. Alertas o mensajes de consola.
  - b. Excepciones de registro del sistema.
  - c. Alarmas de gestión de red.
  - d. Alarmas originadas por el sistema de control del acceso.
- e) Cambios e intentos de cambio en la configuración y los controles de la seguridad del sistema.

La frecuencia con la cual se revisan los resultados de las actividades de monitoreo debería depender de los riesgos involucrados. Los factores de riesgo que se deberían considerar incluyen:

- a) Importancia de los procesos de aplicación.
- b) Valor, sensibilidad e importancia de la información implicada.
- c) Experiencia previa de infiltración o uso inadecuado del sistema, y frecuencia de aprovechamiento de las vulnerabilidades.
- d) Extensión de la interconexión del sistema (particularmente en redes públicas).
- e) Registro del servicio de operación que se desactiva.

### **Información adicional**

Es necesario el uso de procedimientos de monitoreo para garantizar que los usuarios únicamente ejecutan actividades autorizadas explícitamente.

La revisión del registro implica la comprensión de las amenazas enfrentadas por el sistema y la forma en que se pueden originar.

### **2.2.5.10.3 PROTECCIÓN DEL REGISTRO DE LA INFORMACIÓN**

#### **Control**

El registro del servicio y la información se deberían proteger contra el acceso o la manipulación no autorizados.

#### **Guía de implementación**

Los controles deberían tener como objeto la protección contra cambios no autorizados y problemas operativos con el registro del servicio incluyendo.

- a) Alteraciones en los tipos de mensaje que se registran.
- b) Archivos de registro que se editan o eliminan.
- c) Capacidad de almacenamiento que se excede del archivo del registro, lo que produce ya sea en la falla para grabar eventos o sobre-escritura de eventos grabados anteriormente.

Puede ser necesario archivar algunos registros para auditoria como parte de la política de retención de registros o debido a los requisitos para recolectar y conservar evidencia.

#### **Información adicional**

Los registros del sistema a menudo contienen un gran volumen de información, mucha de la cual no tiene relación con el monitoreo de la seguridad.

Para facilitar la identificación de los eventos significativos para propósitos del monitoreo de la seguridad, se debería considerar el copiado automático de los tipos apropiados de mensaje en un segundo registro y / o el uso de utilidades del sistema adecuadas o de herramientas de auditoria para realizar la interrogación y racionalización del archivo.

Es necesario proteger los registros del sistema porque si sus datos se pueden modificar o eliminar, su existencia puede crear un sentido falso de la seguridad.



#### **2.2.5.10.4 REGISTROS DEL ADMINISTRADOR Y DEL OPERADOR**

##### **Control**

Se deberían registrar las actividades tanto del operador como del administrador del sistema.

##### **Guía de implementación**

Los registros deberían incluir:

- a) La hora en que ocurrió el evento (exitoso o fallido).
- b) Información sobre el evento (por ejemplo archivos manipulados) o la falla (por ejemplo errores que se presentaron y acciones correctivas que se tomaron).
- c)Cuál cuenta y cuál administrador u operador estuvo involucrado.
- d) Cuales procesos estuvieron implicados.

Los registros del operador y del administrador del sistema se deberían revisar con regularidad.

##### **Información adicional**

Se puede emplear un sistema de detección de intrusos que este fuera del control del sistema y de los administradores de red para monitorear el cumplimiento de las actividades de sistema y de la administración de la red.

#### **2.2.5.10.5 REGISTRO DE FALLAS**

##### **Control**

Las fallas se deberían registrar y analizar, y se deberían tomar las acciones adecuadas.

## **Guía de Implementación**

Se deberían registrar las fallas reportadas por los usuarios o por los programas del sistema relacionadas con problemas de procesamiento de la información o con los sistemas de comunicación. Deberían existir reglas claras para el manejo de las fallas reportadas, incluyendo:

- a) Revisión de los registros de fallas para garantizar que éstas se han resuelto satisfactoriamente.
- b) Revisión de las medidas correctivas para garantizar que no se han puesto en peligro los controles y que la acción tomada está totalmente autorizada.
- c) Se debería asegurar que el registro de errores está habilitado, si está disponible esta función del sistema.

## **Información adicional**

El registro de errores y de fallas puede tener impacto en el desempeño del sistema. Dicho registro debería ser habilitado por personal competente y el nivel necesario de registro para sistemas individuales se debería determinar mediante una evaluación de riesgos, teniendo en cuenta el deterioro del desempeño.

### **2.2.5.10.6 SINCRONIZACIÓN DE RELOJES**

#### **Control**

Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la organización o del dominio de la seguridad deberían estar sincronizados con una fuente de tiempo exacta y acordada.

#### **Guía de implementación**

Cuando un computador o un dispositivo de comunicaciones tiene la capacidad para operar un reloj en tiempo real, dicho reloj se debería establecer como el estándar acordado, por ejemplo el tiempo coordinado universal (UTC) o el tiempo estándar local.

Debido a que se sabe que algunos relojes varían con el paso del tiempo, debería existir un procedimiento que verifique y corrija cualquier variación significativa.

La interpretación correcta del formato fecha/hora es importante para garantizar que la marca de tiempo refleja la fecha/hora real. Es conveniente tener en cuenta las especificaciones locales (por ejemplo el horario de verano).

### **Información adicional**

La configuración correcta de los relojes del computador es importante para garantizar la exactitud de los registros para auditoría, lo cual puede ser necesario para las investigaciones o como evidencia en casos disciplinarios o legales. Los registros inexactos de auditoría pueden dificultar dichas investigaciones y deteriorar la credibilidad de la evidencia. Se puede utilizar un reloj sincronizado a un reloj atómico nacional el cual es tomado como reloj maestro para los sistemas de acceso. También se puede usar un protocolo de tiempo de red para mantener todos los servidores en sincronización con el reloj maestro.

## **2.2.6 CONTROL DEL ACCESO**

### **2.2.6.1 REQUISITOS DEL NEGOCIO PARA EL CONTROL DEL ACCESO**

Controlar el acceso a la información.

El acceso a la información, a los servicios de procesamiento de información y a los procesos del negocio se debería controlar con base en los requisitos de la seguridad y del negocio.

Las reglas para el control del acceso deberían tener en cuenta las políticas de distribución y autorización de la información.

### **2.2.6.1.1 POLÍTICA DE CONTROL DE ACCESO**

#### **Control**

Se debería establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso.

#### **Guía de implementación**

Las reglas y los derechos para el control del acceso para cada usuario o grupo de usuarios se deberían establecer con claridad en una política de control del acceso. Los controles del acceso son tanto lógicos como físicos y se deberían considerar en conjunto.

A los usuarios y a los proveedores de servicios se les debería brindar una declaración clara de los requisitos del negocio que deben cumplir los controles del acceso.

La política debería considerar los siguientes aspectos:

- a) Requisitos de la seguridad de las aplicaciones individuales del negocio.
- b) Identificación de toda la información relacionada con las aplicaciones del negocio y los riesgos a los que se enfrenta la información.
- c) Políticas para la distribución y autorización de la información, como por ejemplo la necesidad de conocer el principio y los niveles de la seguridad y la clasificación de la información.
- d) Consistencia entre el control del acceso y las políticas de clasificación de la información de sistemas y redes diferentes.
- e) Legislación pertinente y obligaciones contractuales relacionadas con la protección del acceso a los datos o los servicios.
- f) Perfiles estándar de acceso de usuario para funciones laborales comunes en la organización.
- g) Gestión de los derechos de acceso en un entorno distribuido y con red que reconozca todos los tipos de conexiones posibles.

- h) Distribución de las funciones de control de acceso, por ejemplo solicitud de acceso, autorización del acceso, administración del acceso.
- i) Requisitos para la autorización formal de las solicitudes de acceso.
- j) Requisitos para la revisión periódica de los controles de acceso.
- k) Retiro de los derechos de acceso.

### **Información adicional**

Se recomienda cuidado al especificar las reglas de control de acceso para considerar:

- a) Diferenciación entre reglas que siempre se deben hacer cumplir y directrices que son opcionales o condicionales.
- b) Establecimiento de reglas basadas en la premisa "En general, todo está prohibido, a menos que esté expresamente permitido" y no en la regla más débil de " En general, todo está permitido, a menos que esté expresamente prohibido".
- c) Cambios en las etiquetas de la información que son iniciados automáticamente por los servicios de procesamiento de información y aquellos iniciados a discreción del usuario.
- d) Cambios en los permisos de usuario que son iniciados automáticamente por los servicios de procesamiento de información y aquellos iniciados por un administrador.
- e) Reglas que requieren aprobación específica antes de su promulgación y aquellas que no.

Las reglas de control de acceso deberían tener soporte de procedimientos formales y de responsabilidades claramente definidas.

## **2.2.6.2 GESTIÓN DEL ACCESO DE USUARIOS**

Asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información.

Se deberían establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información.

Los procedimientos deberían comprender todas las fases del ciclo de vida del acceso del usuario, desde el registro inicial de los usuarios nuevos hasta la cancelación final del registro de usuarios que ya no requieren acceso a los servicios y sistemas de información.

Se debería poner atención especial, según el caso, a la necesidad de controlar la asignación de derechos de acceso privilegiado que permiten a los usuarios anular los controles del sistema.

### **2.2.6.2.1 REGISTRO DE USUARIOS**

#### **Control**

Debería existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.

#### **Guía de implementación**

El procedimiento de control del acceso para el registro y cancelación de usuarios debería incluir:

- a) Uso de la identificación única de usuario (ID) para permitir que los usuarios queden vinculados y sean responsables de sus acciones. el uso de identificadores (ID) de grupo únicamente se debería permitir cuando son necesarios por razones operativas o del negocio, y deberían estar aprobados y documentados.

- b) Verificación de que el usuario tenga autorización del responsable del sistema para el uso del sistema o servicio de información, también pueden ser conveniente que la dirección apruebe por separado los derechos de acceso.
- c) Verificación de que el nivel de acceso otorgado sea adecuado para los propósitos del negocio y sea consistente con la política de la seguridad de la organización, es decir, no pone en peligro la distribución de funciones.
- d) Dar a los usuarios una declaración escrita de sus derechos de acceso.
- e) Exigir a los usuarios firmar declaraciones que indiquen que ellos entienden las condiciones del acceso.
- f) Asegurar que los proveedores del servicio no otorguen el acceso hasta que se hayan terminado los procedimientos de autorización.
- g) Mantenimiento de un registro formal de todas las personas registradas para usar el servicio.
- h) Retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han cambiado de función, de trabajo o que han dejado la organización.
- i) Verificar, retirar o bloquear periódicamente las identificaciones (ID) y cuentas redundantes de usuarios.
- j) Garantizar que las identificaciones (ID) de usuario redundantes no se otorgan a otros usuarios.

### **Información adicional**

Se debería considerar el establecimiento de roles de acceso de usuario basadas en los requisitos del negocio que incluyan un número de derechos en perfiles típicos de acceso de usuario. Las solicitudes y revisiones de acceso se gestionan más fácilmente en el ámbito de dichas funciones que en el ámbito de derechos particulares.

Es conveniente considerar la inclusión de cláusulas en los contratos del personal y de los servicios que especifiquen las sanciones si el personal o los agentes del servicio intentan el acceso no autorizado.

## 2.2.6.2.2 GESTIÓN DE PRIVILEGIOS

### Control

Se debería restringir y controlar la asignación y el uso de privilegios. Guía de implementación

Los sistemas de usuario múltiple que requieren protección contra el acceso no autorizado deberían controlar la asignación de privilegios a través de un proceso formal de autorización.

Se recomienda tener en cuenta los siguientes elementos:

- a) Se deberían identificar los usuarios y sus privilegios de acceso asociados con cada producto del sistema, como sistema operativo, sistema de gestión de bases de datos y aplicaciones.
- b) Se deberían asignar los privilegios a los usuarios sobre los principios de necesidad de uso y evento por evento, y de manera acorde con la política de control de acceso, es decir, el requisito mínimo para su función, sólo cuando sea necesario.
- c) Se deberían conservar un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no se deberían otorgar hasta que el proceso de autorización esté completo.
- d) Es conveniente promover el desarrollo y empleo de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.
- e) Se recomienda promover también el desarrollo y empleo de programas que eviten la necesidad de funcionar con privilegios.
- f) Los privilegios se deberían asignar a un identificador de usuario (ID) diferente a los utilizados para el uso normal del negocio.



## **Información adicional**

El uso no apropiado de los privilegios de administración del sistema (cualquier característica o servicio de un sistema que permita al usuario anular los controles del sistema o de la aplicación) puede ser un factor contribuyente importante a las fallas o vulnerabilidades del sistema.

### **2.2.6.2.3 GESTIÓN DE CONTRASEÑAS PARA USUARIOS**

#### **Control**

La asignación de contraseñas se debería controlar a través de un proceso formal de gestión.

#### **Guía de implementación**

El proceso debería incluir los siguientes requisitos:

- a) Se debería exigir a los usuarios la firma de una declaración para mantener confidenciales las contraseñas personales y conservar las contraseñas de grupo únicamente entre los miembros de éste. esta declaración firmada se podría incluir en los términos y condiciones laborales.
- b) Cuando se exige a los usuarios mantener sus propias contraseñas, inicialmente se les debería suministrar una contraseña temporal segura que estén forzados a cambiar inmediatamente.
- c) Establecer procedimientos para verificar la identidad de un usuario antes de proporcionarle una contraseña temporal, de reemplazo o nueva.
- d) Las contraseñas temporales se deberían suministrar de forma segura a los usuarios. se recomienda evitar mensajes de correo electrónico de terceras partes o sin protección (texto claro).
- e) Las contraseñas temporales deberían ser únicas para un individuo y no ser descifrables.

- f) Los usuarios deberían confirmar la entrega de las contraseñas.
- g) Las contraseñas nunca se deberían almacenar en sistemas de computador en un formato no protegido.
- h) Las contraseñas predeterminadas por el proveedor se deberían cambiar inmediatamente después de la instalación de los sistemas o del software.

### **Información adicional**

Las contraseñas son un medio común de verificación de la identidad de un usuario antes de darle acceso a un sistema o servicio de información de acuerdo con la autorización del usuario.

Según el caso, es recomendable considerar otras tecnologías disponibles para la identificación y autenticación del usuario tales como biométricos, (verificación de huella digital, verificación de firma) y el uso de tokens de autenticación, (tarjetas inteligentes).

#### **2.2.6.2.4 REVISIÓN DE LOS DERECHOS DE ACCESO DE LOS USUARIOS**

##### **Control**

La dirección debería establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.

##### **Guía de implementación**

Se recomienda que en la revisión de los derechos de acceso se consideren las siguientes directrices:

- a) Los derechos de acceso de los usuarios se deberían revisar a intervalos regulares, por ejemplo cada seis meses y después de cada cambio, como por ejemplo promoción, cambio a un cargo en un nivel inferior, o terminación del contrato laboral.

- b) Los derechos de acceso de usuarios se deberían revisar y reasignar cuando hay cambios de un cargo a otro dentro de la misma organización.
- c) Es recomendable revisar las autorizaciones para derechos de acceso privilegiado a intervalos más frecuentes, por ejemplo cada tres meses.
- d) Se debería verificar la asignación de privilegios a intervalos regulares para garantizar que no se obtienen privilegios no autorizados.
- e) Los cambios en las cuentas privilegiadas se deberían registrar para su revisión periódica.

### **Información adicional**

Es necesario revisar con regularidad los derechos de acceso de los usuarios para mantener un control eficaz del acceso a los datos y a los servicios de información.

### **2.2.6.3 RESPONSABILIDADES DE LOS USUARIOS**

Evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información.

La cooperación de los usuarios autorizados es esencial para la eficacia de la seguridad.

Se debería concientizar a los usuarios sobre sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular con relación al uso de contraseñas y a la seguridad del equipo del usuario.

Es recomendable implementar una política de escritorio y pantalla despejados para reducir el riesgo de acceso no autorizado o daño de reportes, medios y servicios de procesamiento de información.

### **2.2.6.3.1 USO DE CONTRASEÑAS**

#### **Control**

Se debería exigir a los usuarios el cumplimiento de buenas prácticas de la seguridad en la selección y el uso de las contraseñas.

#### **Guía de implementación**

Todos los usuarios deberían:

- a) Mantener la confidencialidad de las contraseñas.
- b) Evitar conservar registros (por ejemplo en papel, archivos de software o dispositivos manuales) de las contraseñas, a menos que éstas se puedan almacenar de forma segura y el método de almacenamiento esté aprobado.
- c) Cambiar las contraseñas siempre que haya indicación de puesta en peligro del sistema o de la contraseña.
- d) Seleccionar contraseñas de calidad con longitud mínima suficiente que:
  - a. Sean fáciles de recordar.
  - b. No se basen en algo que alguien pueda adivinar fácilmente o usando información relacionada con la persona, por ejemplo nombre, números telefónicos, fechas de cumpleaños, etc.
  - c. No sean vulnerables al ataque de diccionarios (es decir, que no consistan en palabras incluidas en diccionarios).
  - d. No tengan caracteres idénticos consecutivos, que no sean todos numéricos ni todos alfabéticos.

- e) Cambiar las contraseñas a intervalos regulares o con base en el número de accesos (las contraseñas para cuentas privilegiadas se deberían cambiar con más frecuencia que las contraseñas normales) y evitar la reutilización de contraseñas antiguas.
- f) Cambiar las contraseñas temporales en el primer registro de inicio.
- g) No incluir contraseñas en ningún proceso de registro automatizado, por ejemplo almacenadas en un macro o en una clave de función.
- h) No compartir las contraseñas de usuario individuales.
- i) No utilizar la misma contraseña para propósitos del negocio y para los que no lo son.

Si los usuarios necesitan acceso a múltiples servicios, sistemas o plataformas y se les exige conservar múltiples contraseñas separadas, se les debería advertir que pueden usar una sola contraseña de calidad para todos los servicios cuando se les garantiza que se ha establecido un nivel razonable de protección para almacenar la contraseña en cada servicio, sistema o plataforma.

### **Información adicional**

La gestión de los sistemas de ayuda del escritorio auxiliar que tratan con las contraseñas perdidas u olvidadas necesita cuidado especial puesto que también puede ser un medio de ataque al sistema de contraseña.

#### **2.2.6.3.2 EQUIPO DE USUARIO DESATENDIDO**

##### **Control**

Los usuarios deberían asegurarse de que los equipos desatendidos tengan protección apropiada.

## **Guía de implementación**

Se debería concientizar a los usuarios sobre los requisitos y los procedimientos de la seguridad para proteger los equipos desatendidos, así como sobre sus responsabilidades en la implementación de dicha protección. Se debería advertir a los usuarios sobre:

- a) Terminar las sesiones activas cuando finalice, a menos que se puedan asegurar por medio de un mecanismo de bloqueo, como un protector de pantalla protegido por contraseña.
- b) Realizar el registro de cierre en computadoras principales, servidores y computadores personales de oficina al terminar la sesión (es decir, no sólo apagar el interruptor de la pantalla del computador o terminal).
- c) Cuando no están en uso, asegurar los computadores personales o los terminales contra el uso no autorizado mediante una clave de bloqueo o un control equivalente como, por ejemplo, el acceso por contraseña.

## **Información adicional**

Los equipos instalados en las áreas de usuario, por ejemplo las estaciones de trabajo o los servidores de archivo, pueden requerir protección específica contra el acceso no autorizado cuando se dejen desatendidos durante periodos prolongados.

### **2.2.6.3.3 POLÍTICA DE ESCRITORIO DESPEJADO Y DE PANTALLA DESPEJADA**

#### **Control**

Se debería adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información.

## **Guía de implementación**

En la política de escritorio despejado y pantalla despejada se deberían considerar las clasificaciones de la información, los requisitos legales y contractuales, los riesgos correspondientes y los aspectos culturales de la organización. Es recomendable tener presentes las siguientes directrices:

- a) Cuando no se requiere la información sensible o crítica del negocio, como por ejemplo los medios de almacenamiento electrónicos o en papel, se debería asegurar bajo llave (idealmente una caja fuerte, un gabinete u otro mueble de la seguridad), especialmente cuando la oficina está vacía.
- b) las sesiones de los computadores y los terminales se deberían cerrar o proteger con un mecanismo de bloqueo de pantalla y de teclado controlado por una contraseña, un token o un mecanismo similar de autenticación de usuario cuando no están atendidos, y se deberían proteger mediante bloqueos de clave, contraseñas u otros controles cuando no se estén utilizando.
- c) Se deberían proteger los puntos de entrada y salida de correo y las máquinas de facsímil desatendidas.
- d) Es conveniente evitar el uso no autorizado de fotocopiadoras y otra tecnología de reproducción (por ejemplo, escáneres, cámaras digitales, etc.).
- e) Los documentos que contengan información sensible o clasificada se deberían retirar inmediatamente de las impresoras.

## **Información adicional**

Una política sobre escritorio despejado/pantalla despejada reduce los riesgos de acceso no autorizado, pérdida y daño de la información durante y fuera de las horas laborales normales.

Las cajas fuertes u otras formas de almacenamiento seguro también podrían proteger la información almacenada allí contra desastres como incendio, terremoto, inundación o explosión.

Se debería pensar en la utilización de impresoras con función de código de pines (pin code) de forma que quien inicia la impresión sea el único que pueda obtenerla y únicamente cuando esté cerca de la impresora.

#### **2.2.6.4 CONTROL DE ACCESO A LAS REDES**

Evitar el acceso no autorizado a los servicios en red.

Es recomendable controlar el acceso a los servicios en red, tanto internos como externos.

El acceso de los usuarios a las redes y a los servicios de red no debería comprometer la seguridad de los servicios de red garantizando que:

- a) Existen interfaces apropiadas entre la red de la organización y las redes que pertenecen a otras organizaciones, y las redes públicas.
- b) Se aplican mecanismos adecuados de autenticación para los usuarios y los equipos.
- c) Se exige control de acceso de los usuarios a los servicios de información.

##### **2.2.6.4.1 POLÍTICA DE USO DE LOS SERVICIOS EN RED**

###### **Control**

Los usuarios sólo deberían tener acceso a los servicios para cuyo uso están específicamente autorizados.

###### **Guía de implementación**

Se debería formular una política con respecto al uso de las redes y los servicios de red. Esta política debería abarcar:

- a) Las redes y los servicios de red a los cuales se permiten el acceso.



- b) Los procedimientos de autorización para determinar a quién se le permite el acceso a qué redes y qué servicios en red.
- c) Los controles y procedimientos de gestión para proteger el acceso a las conexiones de red y los servicios de red.
- d) Los medios utilizados para el acceso a las redes y los servicios de red (por ejemplo las condiciones para permitir el acceso a la marcación a un proveedor de servicios de Internet o a un sistema remoto).

La política sobre el uso de los servicios de red debería ser consistente con la política de control de acceso de la organización.

### **Información adicional**

Las conexiones inseguras y no autorizadas a servicios de red pueden afectar a toda la organización. Este control es particularmente importante para las conexiones de red de aplicaciones sensibles o críticas para el negocio o para usuarios en lugares de alto riesgo, por ejemplo en áreas públicas o externas que se hallan fuera del control y la gestión de la seguridad de la organización.

#### **2.2.6.4.2 AUTENTICACIÓN DE USUARIOS PARA CONEXIONES EXTERNAS**

##### **Control**

Se deberían emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos.

##### **Guía de implementación**

La autenticación de usuarios remotos se puede lograr usando, por ejemplo, una técnica con base criptográfica, token de hardware o protocolos de desafío / respuesta. Las posibles implementaciones de dichas técnicas se pueden encontrar en diversas soluciones de red privada virtual (VPN). Las líneas privadas dedicadas también se pueden emplear para brindar aseguramiento de la fuente de las conexiones.

Los procedimientos y controles de devolución de marcación, por ejemplo empleando módems de retorno de marcación, pueden suministrar protección contra conexiones no deseadas o no autorizadas a los servicios de procesamiento de información de la organización. Este tipo de control autentica a los usuarios tratando de establecer una conexión con una red de la organización desde sitios remotos.

Cuando se usa este control, la organización no debería utilizar servicios de red que incluyen envío de llamada o, si lo hacen, deberían desactivar el uso de dichas características para evitar las debilidades asociadas con el envío de llamada. El proceso de devolución de llamada debería garantizar que realmente se produce una desconexión en el lado de la organización. De otro modo, el usuario remoto debería mantener la línea abierta pretendiendo que ha ocurrido la verificación de la devolución de la llamada. Los procedimientos y controles de devolución de la llamada se deberían probar en su totalidad para determinar esta posibilidad.

La autenticación del nodo puede servir como un medio alternativo para la autenticación de grupos de usuarios remotos cuando están conectados a un servicio seguro de computador compartido. Para la autenticación del nodo se pueden emplear las técnicas criptográficas, por ejemplo las basadas en certificados de máquina. Esto forma parte de varias soluciones basadas en la red privada virtual (VPN).

Se deberían implementar controles de autenticación adicionales para controlar el acceso a redes inalámbricas. En particular, es necesario tener cuidado especial en la selección de los controles para redes inalámbricas debido a las grandes oportunidades para la interceptación e inserción no detectadas en el tráfico de la red.

### **Información adicional**

Las conexiones externas suministran un potencial para el acceso no autorizado a la información del negocio, por ejemplo el acceso a los métodos de marcación. Existen diferentes métodos de autenticación, algunos de los cuales proporcionan un mayor grado de protección que otros, como por ejemplo los métodos con base en el uso de técnicas criptográficas que pueden brindar autenticación sólida. Es importante determinar a partir de una evaluación de riesgos el grado necesario de protección. Ello es necesario para la selección adecuada de un método de autenticación.

Un medio para la conexión automática a un computador remoto podría suministrar una forma de obtener acceso no autorizado a una aplicación del negocio. Esto es especialmente importante si la conexión utiliza una red que está fuera del control de la gestión de la seguridad de la organización.

#### **2.2.6.4.3 IDENTIFICACIÓN DE LOS EQUIPOS EN LAS REDES**

##### **Control**

La identificación automática de los equipos se debería considerar un medio para autenticar conexiones de equipos y ubicaciones específicas.

##### **Guía de implementación**

Se puede usar la identificación del equipo, si es importante que la comunicación únicamente se pueda iniciar desde un equipo o lugar específico. Un identificador en el equipo o acoplado a éste se puede usar para indicar si está permitido que este equipo se conecte a la red. Estos identificadores deberían indicar con claridad a qué red está permitido conectar el equipo, si existe más de una red y si estas redes tienen sensibilidad diferente. Puede ser necesario considerar la protección física del equipo para mantener la seguridad del identificador de éste.

##### **Información adicional**

Este control se puede complementar con otras técnicas para autenticar el usuario del equipo. La identificación del equipo se puede aplicar en adición a la autenticación del usuario.

#### **2.2.6.4.4 PROTECCIÓN DE LOS PUERTOS DE CONFIGURACIÓN Y DIAGNÓSTICO REMOTO**

##### **Control**

El acceso lógico y físico a los puertos de configuración y de diagnóstico debería estar controlado.

## **Guía de implementación**

Los controles potenciales para el acceso a los puertos de diagnóstico y configuración incluyen el uso de un bloqueo de clave y procedimientos de soporte para controlar el acceso físico al puerto. Un ejemplo de un procedimiento de soporte es garantizar que los puertos de diagnóstico y configuración sólo sean accesibles mediante acuerdo entre el administrador del servicio de computador y el personal de soporte de hardware / software que requiere el acceso.

Los puertos, servicios y prestaciones similares instaladas en un servicio de computador o de red, que no se requieren específicamente para la funcionalidad del negocio, se deberían inhabilitar o retirar.

## **Información adicional**

Muchos sistemas de computador, sistemas de red y sistemas de comunicación se instalan en un sitio de configuración o de diagnóstico remoto para ser utilizados por los ingenieros de mantenimiento. Si no están protegidos, estos puertos de diagnóstico son un medio para el acceso no autorizado.

### **2.2.6.4.5 SEPARACIÓN EN LAS REDES**

#### **Control**

En las redes se deberían separar los grupos de servicios de información, usuarios y sistemas de información.

#### **Guía de implementación**

Un método para el control en las redes grandes es dividir las en dominios lógicos de red separados, por ejemplo, dominios de red internos de la organización y dominios de red extremos, cada uno protegido por un perímetro de la seguridad definido.

Se puede aplicar un conjunto graduado de controles en diferentes dominios lógicos de red para separar aún más los entornos de la seguridad de la red, por ejemplo los sistemas de acceso público, las redes internas y los activos críticos. Los dominios se deberían definir con base en una evaluación de riesgos y en los diferentes requisitos de la seguridad en cada uno de los dominios.

Se puede implementar un perímetro de red instalando una puerta de enlace (Gateway) seguro entre las dos redes que se van a interconectar para controlar el acceso y el flujo de información entre los dos dominios. Esta puerta de enlace (Gateway) se debería configurar para filtrar el tráfico entre estos dominios y para bloquear el acceso no autorizado, según la política de control de acceso de la organización. Un ejemplo de este tipo de puerta de enlace (gateway) es lo que se conoce comúnmente como barrera de fuego (firewall). Otro método para apartar los dominios lógicos separados es restringir el acceso a la red usando redes privadas virtuales para grupos de usuarios dentro de la organización.

Las redes también se pueden separar utilizando la funcionalidad del dispositivo de red, por ejemplo la conmutación IP. Los dominios separados se pueden implementar entonces controlando los flujos de datos de la red usando las capacidades de enrutamiento/conmutación, como por ejemplo las listas de control de acceso.

Los criterios para separar las redes en dominios se deberían basar en la política de control de acceso y en los requisitos de acceso y deberían tener en cuenta los costos relativos y el impacto en el desempeño por la incorporación de tecnología conveniente de puerta de enlace (Gateway) o de enrutamiento de red.

Además, la separación de las redes se debería basar en el valor y la clasificación de la información almacenada o procesada en la red, los niveles de confianza o los lineamientos del negocio con el fin de reducir el impacto total de una interrupción del servicio.

También se debería pensar en la separación de las redes inalámbricas procedentes de redes internas y privadas. Puesto que los perímetros de las redes inalámbricas no están bien definidos, es recomendable llevar a cabo una evaluación de riesgos en tales casos para identificar los controles (por ejemplo, autenticación sólida, métodos criptográficos y selección de frecuencia) para mantener la separación de la red.

## **Información adicional**

Las redes se extienden cada vez más allá de las fronteras tradicionales de la organización, ya que se forman sociedades de negocios que pueden requerir la interconexión o compartir el procesamiento de información y las prestaciones de la red.

Tal extensión puede incrementar el riesgo no autorizado a los sistemas de información existentes que utilizan la red, algunos de los cuales pueden requerir protección contra otros usuarios de la red debido a su sensibilidad o importancia.

### **2.2.6.4.6 CONTROL DE CONEXIÓN A LAS REDES**

#### **Control**

Para redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la organización, se debería restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control de acceso y los requisitos de aplicación del negocio.

#### **Guía de implementación**

Los derechos de acceso a la red de los usuarios se deberían mantener y actualizar según se requiera a través de la política de control de acceso.

La capacidad de conexión de los usuarios se puede restringir a través de puertas de enlace (gateway) de red que filtren el tráfico por medio de tablas o reglas predefinidas.

Los siguientes son algunos ejemplos de aplicaciones a las cuales se deberían aplicar restricciones:

- a) Mensajería, por ejemplo, el correo electrónico.
- b) Transferencia de archivos.
- c) Acceso interactivo.

d) Acceso a las aplicaciones.

Es conveniente tomar en consideración el enlace de los derechos de acceso a la red con algunas horas del día o fechas.

### **Información adicional**

La política de control del acceso puede exigir la incorporación de controles para restringir la capacidad de conexión de los usuarios a redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la organización.

#### **2.2.6.4.7 CONTROL DEL ENRUTAMIENTO EN LA RED**

##### **Control**

Se deberían implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control de acceso de las aplicaciones del negocio.

##### **Guía de implementación**

Los controles de enrutamiento se deberían basar en mecanismos de verificación para las direcciones fuente /destino válidos.

Las puertas de enlace (Gateway) de la seguridad se pueden usar para validar la dirección fuente/destino en los puntos de control de las redes interna y externa, si se emplean tecnologías proxy y/o de traducción de dirección de red. Quienes desarrollan la implementación deberían ser conscientes de las fortalezas y deficiencias de los mecanismos desplegados. Los requisitos para el control del enrutamiento en la red se deberían basar en la política de control de acceso.

## **Información adicional**

Las redes compartidas, especialmente aquellas que van más allá de las fronteras de la organización, pueden requerir controles adicionales de enrutamiento. Esto se aplica particularmente cuando las redes son compartidas por usuarios de terceras partes (que no pertenecen a la organización).

### **2.2.6.5 CONTROL DE ACCESO AL SISTEMA OPERATIVO**

Evitar el acceso no autorizado a los sistemas operativos.

Se recomienda utilizar medios de la seguridad para restringir el acceso de usuarios no autorizados a los sistemas operativos. Tales medios deberían tener la capacidad para:

- a) Autenticar usuarios autorizados, de acuerdo con una política definida de control de acceso.
- b) Registrar intentos exitosos y fallidos de autenticación del sistema.
- c) Registrar el uso de privilegios especiales del sistema.
- d) Emitir alarmas cuando se violan las políticas de la seguridad del sistema.
- e) Suministrar medios adecuados para la autenticación.
- f) Cuando sea apropiado, restringir el tiempo de conexión de los usuarios.

#### **2.2.6.5.1 PROCEDIMIENTOS DE REGISTRO DE INICIO SEGURO**

##### **Control**

El acceso a los sistemas operativos se debería controlar mediante un procedimiento de registro de inicio seguro.



## Guía de implementación

El procedimiento de registro en un sistema operativo debería estar diseñado para minimizar la oportunidad de acceso no autorizado. Por lo tanto, el procedimiento de registro de inicio debería divulgar información mínima sobre el sistema para evitar suministrar asistencia innecesaria a un usuario no autorizado. Un buen procedimiento de registro de inicio debería cumplir los siguientes aspectos:

- a) No mostrar identificadores de aplicación ni de sistema hasta que el proceso de registro de inicio se haya completado exitosamente.
- b) Mostrar una advertencia de notificación general indicando que sólo deberían tener acceso al computador los usuarios autorizados.
- c) No suministrar mensajes de ayuda durante el procedimiento de registro de inicio que ayuden a un usuario no autorizado.
- d) Validar la información de registro de inicio únicamente al terminar todos los datos de entrada. Si se presenta una condición de error, el sistema no debería indicar qué parte de los datos es correcta o incorrecta.
- e) Limitar la cantidad de intentos permitidos de registro de inicio, por ejemplo tres intentos, y considerar:
  - a. Registrar intentos exitosos y fallidos.
  - b. Forzar un tiempo de dilación antes de permitir intentos adicionales del registro de inicio o de rechazar los intentos adicionales sin autorización específica.
  - c. Desconectar las conexiones de enlaces de datos.
  - d. Enviar un mensaje de alarma a la consola del sistema si se alcanza la cantidad máxima de intentos de registro de inicio.
  - e. Establecer la cantidad de reintentos de contraseña junto con la longitud mínima de ella y el valor del sistema que se protege.

- f) Limitar el tiempo máximo y mínimo permitido para el procedimiento de registro de inicio. Si se excede, el sistema debería finalizar esta operación.
- g) Mostrar la siguiente información al terminar un registro de inicio exitoso:
- h) Fecha y hora del registro de inicio exitoso previo.
- i) Detalles de los intentos fallidos de registro de inicio desde el último registro exitoso.
- j) No mostrar la contraseña que se introduce o considerar esconder los caracteres mediante símbolos.
- k) No transmitir contraseñas en texto claro en la red.

### **Información adicional**

Si las contraseñas se transmiten en texto claro durante la sesión de registro de inicio pueden ser capturadas en la red por un programa "husmeador" de red.

## **2.2.6.5.2 IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS**

### **Control**

Todos los usuarios deberían tener un identificador único (ID del usuario) para su uso personal, y se debería elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario.

### **Guía de implementación**

Este control se debería aplicar a todos los tipos de usuarios (incluyendo el personal de soporte técnico, operadores, administradores de red, programadores de sistemas y administradores de bases de datos).

Los identificadores de usuario (ID) se deberían utilizar para rastrear las actividades de la persona responsable. Las actividades de usuarios regulares no se deberían realizar desde cuentas privilegiadas.

En circunstancias excepcionales, cuando existe un beneficio claro para el negocio, se puede usar un identificador de usuario compartido para un grupo de usuarios o un trabajo específico.

La aprobación por la dirección debería estar documentada para dichos casos. Se pueden requerir controles adicionales para mantener la responsabilidad.

Sólo se deberían permitir los identificadores (ID) de usuario genéricos para uso de un individuo si existen funciones accesibles o si no es necesario rastrear las acciones ejecutadas por el identificador (por ejemplo el acceso de sólo lectura), o cuando no hay controles establecidos (por ejemplo cuando la contraseña para un identificador genérico sólo se emite para un personal a la vez y el registro de tal caso).

Cuando se requiere verificación de identidad y autenticación sólidas, se deberían utilizar métodos alternos a la contraseña, como los medios criptográficos, las tarjetas inteligentes, token o medios biométricos.

### **Información adicional**

Las contraseñas son una forma muy común de identificar y autenticar con base en un secreto que sólo conoce el usuario. Lo mismo se puede lograr con medios criptográficos y protocolos de autenticación. La fortaleza de la identificación y autenticación del usuario debería ser adecuada a la sensibilidad de la información a la que se tiene acceso.

Objetos tales como los tokens de memoria o las tarjetas inteligentes que poseen los usuarios también se pueden usar para la identificación y la autenticación. Las tecnologías de autenticación biométrica que utilizan características o atributos únicos de un individuo también se pueden usar para autenticar la identidad de una persona. Una combinación de tecnologías y mecanismos enlazados con seguridad producirá una autenticación sólida.

### **2.2.6.5.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS**

#### **Control**

Los sistemas para la gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.

#### **Guía de implementación**

Un sistema de gestión de contraseñas debería:

- a) Hacer cumplir el uso de identificadores de usuario (ID) individual y de contraseñas para conservar la responsabilidad.
- b) Permitir a los usuarios la selección y el cambio de sus contraseñas e incluir un procedimiento de confirmación para tener en cuenta los errores en los ingresos.
- c) Imponer una elección de contraseñas de calidad.
- d) Imponer cambios de contraseña.
- e) Forzar a los usuarios a cambiar las contraseñas temporales en el primer registro de inicio.
- f) Conservar un registro de las contraseñas de usuario previas y evitar su reutilización.
- g) No mostrar contraseñas en la pantalla cuando se hace su ingreso.
- h) Almacenar los archivos de contraseñas separadamente de los datos del sistema de aplicación.
- i) Almacenar y transmitir las contraseñas en formatos protegidos (por ejemplo encriptadas o codificadas).

## **Información adicional**

Las contraseñas son un mecanismo principal para validar una autoridad del usuario para tener acceso a un servicio de computador.

Algunas aplicaciones requieren la asignación de contraseñas de usuario por parte de una autoridad independiente, en tales casos, no se aplican los literales b), d) y e) indicados en la directriz anterior. En la mayoría de los casos, las contraseñas son seleccionadas y conservadas por los usuarios.

### **2.2.6.5.4 USO DE LAS UTILIDADES DEL SISTEMA CONTROL**

Se debería restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación.

#### **Guía de aplicación**

Se recomienda considerar la siguiente directriz para el uso de las utilidades del sistema:

- a) Uso de procedimientos de identificación, autenticación y autorización para las utilidades del sistema.
- b) Separación de las utilidades del sistema del software de aplicaciones,
- c) Limitación del uso de las utilidades del sistema a la cantidad mínima viable de usuarios de confianza autorizados.
- d) Autorización del uso ad hoc de las utilidades del sistema.
- e) Limitación de la disponibilidad de las utilidades del sistema, por ejemplo para la duración de un cambio autorizado.
- f) Registro de todo uso de las utilidades del sistema.
- g) Definición y documentación de los niveles de autorización para las utilidades del sistema.

- h) Retiro o inhabilitación de todas las utilidades o el software del sistema basado en software innecesario.
- i) No poner a disposición las utilidades del sistema a usuarios que tengan acceso a aplicaciones en sistemas en donde se requiere distribución de funciones.

### **Información adicional**

La mayoría de las instalaciones de computador tiene uno o más programas de utilidades del sistema que pueden anular los controles del sistema y de la aplicación.

### **2.2.6.5.5 TIEMPO DE INACTIVIDAD DE LA SESIÓN**

#### **Control**

Las sesiones inactivas se deberían suspender después de un periodo definido de inactividad.

#### **Guía de implementación**

Un tiempo de inactividad debería despejar la pantalla de sesión y más tarde, cerrar tanto la sesión de la aplicación como la de red después de un periodo definido de inactividad. La dilación del tiempo de inactividad debería reflejar los riesgos de la seguridad del área, la clasificación de la información que se maneja y las aplicaciones que se utilizan, así como los riesgos relacionados con los usuarios del equipo.

Algunos sistemas pueden suministrar una forma limitada de utilidad de tiempo de inactividad la cual despeja la pantalla y evita el acceso no autorizado, pero no cierra las sesiones de aplicación ni de red.

#### **Información adicional**

Este control es importante particularmente en lugares de alto riesgo, los cuales incluyen áreas públicas o externas fuera de la gestión de la seguridad de la organización. Las sesiones se deberían cerrar para evitar el acceso de personas no autorizadas y negar ataques al servicio.

#### **2.2.6.5.6 LIMITACIÓN DEL TIEMPO DE CONEXIÓN**

##### **Control**

Se deberían utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo.

##### **Guía de implementación**

Se deberían tener en cuenta los controles de tiempo para las aplicaciones sensibles de computador, especialmente las de lugares de alto riesgo, por ejemplo áreas públicas o externas que están fuera de la gestión de la seguridad de la organización. Los siguientes son algunos ejemplos de estas restricciones:

- a) Uso de espacios de tiempo predeterminados, por ejemplo, para transmisiones de lotes de archivos, o uso de sesiones interactivas de corta duración.
- b) Restricción de los tiempos de conexión a las horas normales de oficina, si no se requiere tiempo extra u operaciones de horario prolongado.
- c) Considerar la repetición de la autenticación a intervalos determinados.

##### **Información adicional**

La limitación del periodo durante el cual se permite la conexión a los servicios de computador reduce la ventana de oportunidad para el acceso no autorizado. La limitación de la duración de las sesiones activas evita que los usuarios mantengan sesiones abiertas para evitar la repetición de la autenticación.

#### **2.2.6.6 CONTROL DE ACCESO A LAS APLICACIONES Y A LA INFORMACIÓN**

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

Se deberían usar medios de la seguridad para restringir el acceso a los sistemas de aplicación y dentro de ellos.

El acceso lógico al software de aplicación y a la información se debería restringir a usuarios autorizados.

Los sistemas de aplicación deberían:

- a) Controlar el acceso de usuarios a la información y a las funciones del sistema de aplicación, de acuerdo con una política definida de control de acceso.
- b) Suministrar protección contra acceso no autorizado por una utilidad, el software del sistema operativo y software malicioso que pueda anular o desviar los controles del sistema o de la aplicación.
- c) No poner en peligro otros sistemas con los que se comparten los recursos de información.

#### **2.2.6.6.1 RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN**

##### **Control**

Se debería restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.

##### **Guía de implementación**

Las restricciones del acceso se deberían basar en los requisitos de las aplicaciones individuales del negocio. La política de control de acceso también debería ser consistente con la política de acceso de la organización.

Se debería considerar la aplicación de las siguientes directrices con el objeto de dar soporte a los requisitos de restricción del acceso:

- a) Proporcionar menús para controlar el acceso a las funciones del sistema de aplicación.



- b) Controlar los derechos de acceso de los usuarios, por ejemplo, leer, escribir, eliminar y ejecutar.
- c) Controlar los derechos de acceso de otras aplicaciones.
- d) Garantizar que los datos de salida de los sistemas de aplicación que manejan información sensible sólo contienen la información pertinente para el uso de la salida y que se envía únicamente a terminales o sitios autorizados. ello debería incluir revisiones periódicas de dichas salidas para garantizar el retiro de la información redundante.

#### **2.2.6.6.2 AISLAMIENTO DE SISTEMAS SENSIBLES**

##### **Control**

Los sistemas sensibles deberían tener un entorno informático dedicado (aislados).

##### **Guía de implementación**

Se deberían considerar los siguientes puntos para el aislamiento de los sistemas sensibles:

- a) La sensibilidad de un sistema de aplicación se debería identificar y documentar explícitamente por parte del responsable de la aplicación.
- b) Cuando una aplicación se ha de ejecutar en un entorno compartido, los sistemas de aplicación con los cuales compartirá recursos y los riesgos correspondientes deberían ser identificados y aceptados por el responsable de la aplicación sensible.

##### **Información adicional**

Algunos sistemas de aplicación son lo suficientemente sensibles a la pérdida potencial que requieren manejo especial. La sensibilidad puede indicar que el sistema de aplicación debería:

- a) Ejecutarse en un computador dedicado, o
- b) Únicamente debería compartir recursos con sistemas de aplicación confiables.

El aislamiento se puede lograr utilizando métodos físicos o lógicos.

### **2.2.6.7 COMPUTACIÓN MÓVIL Y TRABAJO REMOTO**

Garantizar la seguridad de la información cuando se utilizan dispositivos de computación móviles y de trabajo remoto.

La protección necesaria debería estar acorde con los riesgos que originan estas formas específicas de trabajo. Cuando se usa la computación móvil, se deberían tener en cuenta los riesgos de trabajar en un entorno sin protección y aplicar la protección adecuada. En el caso del trabajo remoto, la organización debería aplicar protección en el sitio del trabajo remoto y garantizar que se han establecido las disposiciones adecuadas para esta forma de trabajo.

#### **2.2.6.7.1 COMPUTACIÓN Y COMUNICACIONES MÓVILES**

##### **Control**

Se debería establecer una política formal y se deberían adoptar las medidas de la seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.

##### **Guía de implementación**

Cuando se usan servicios de computación y de comunicaciones móviles, por ejemplo, computadores portátiles livianos (Notebooks), microcomputadores de bolsillo (Palmtops), y computadores portátiles pesados (Laptops), tarjetas inteligentes y teléfonos móviles se debería tener cuidado especial para asegurarse de que la información no se pone en peligro. En la política de computación móvil se deberían considerar los riesgos de trabajar con

En la política de computación móvil se deberían incluir los requisitos para la protección física, los controles de acceso, las técnicas criptográficas, las copias de respaldo y la protección contra virus. Esta política también debería incluir reglas y asesoría sobre la conexión de los servicios móviles a las redes y directrices sobre el uso de estos servicios en lugares públicos.

Es conveniente tener cuidado cuando se utilizan servicios de computación móvil en lugares públicos, salas de reuniones y otras áreas sin protección fuera de las instalaciones de la organización. Se debería establecer la protección para evitar el acceso o la divulgación no autorizados de la información almacenada y procesada por estos servicios, por ejemplo, usando técnicas criptográficas.

Los usuarios de servicios de computación móviles en lugares públicos deberían tener cuidado, para evitar el riesgo de ser observados por personas no autorizadas. Es recomendable establecer procedimientos contra software malicioso y mantenerlos actualizados.

Es conveniente hacer copias de respaldo a intervalos regulares de la información del negocio.

Se debería disponer de equipo para permitir el respaldo rápido y fácil de la información.

Las copias de respaldo deberían tener protección adecuada contra robo o pérdida de información.

La utilización de los servicios móviles conectados a las redes deberían tener una protección idónea. El acceso remoto a la información del negocio a través de redes públicas usando servicios de computación móvil sólo debería tener lugar después de la identificación y la autenticación exitosa y con el establecimiento de los mecanismos adecuados de control del acceso. Los servicios de computación móvil también se deben proteger físicamente contra robo, especialmente cuando se deja, por ejemplo, en los automóviles y otros medios de transporte, habitaciones de hoteles, centros de conferencias y sitios de reuniones.

Es conveniente establecer un procedimiento específico en el que se tengan presentes los requisitos legales, de seguros y otros de la seguridad de la organización para los casos de robo o pérdida de los servicios de computación móvil. El equipo que porta información sensible y/o crítica importante del negocio no se debería dejar desatendido y, cuando sea posible, se debería bloquear con algún medio físico o usar cerraduras especiales para asegurar el equipo.

Se recomienda disponer la formación del personal que utiliza computación móvil para concientizarlo sobre los riesgos adicionales que se originan en este tipo de trabajo y los controles que se deberían implementar.

### **Información adicional**

Las conexiones inalámbricas a red móvil son similares a otros tipos de conexión de red, pero tienen diferencias importantes que se deberían considerar al identificar los controles. Las diferencias típicas son:

- a) Algunos protocolos de la seguridad inalámbrica son inmaduros y tienen debilidades conocidas.
- b) La información almacenada en los computadores móviles puede no tener copias de respaldo debido al ancho de banda de red limitado y/o a que el equipo móvil puede no estar conectado en las horas en las que están programadas las copias de respaldo.

### **2.2.6.7.2 TRABAJO REMOTO**

#### **Control**

Se deberían desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.

## Guía de implementación

Las organizaciones sólo deberían autorizar las actividades de trabajo remoto si están satisfechas con las disposiciones de la seguridad adecuadas y los controles establecidos, y si ellos cumplen la política de la seguridad de la organización.

Es conveniente establecer una protección apropiada del sitio de trabajo remoto contra, por ejemplo, robo del equipo y la información, divulgación no autorizada de información, acceso remoto no autorizado a los sistemas internos de la organización o el uso inadecuado de sus servicios. Las actividades de trabajo remoto deberían estar autorizadas y controladas por la dirección y se debería garantizar la instauración de disposiciones adecuadas para esta forma de trabajo.

Se recomienda considerar los siguientes aspectos:

- a) La seguridad física existente en el sitio de trabajo remoto, tomando en consideración la seguridad física de la edificación y del entorno local.
- b) El entorno físico de trabajo remoto propuesto.
- c) Los requisitos de la seguridad de las comunicaciones, pensando en la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la cual se tendrá acceso y sobrepasar el enlace de comunicación y la sensibilidad del sistema interno.
- d) La amenaza del acceso no autorizado a la información o los recursos por parte de otras personas que usan el mismo espacio, por ejemplo familiares y amigos.
- e) El uso de redes domésticas y los requisitos o restricciones en la configuración de servicios de red inalámbrica.
- f) Las políticas y los procedimientos para evitar disputas con respecto a los derechos de propiedad intelectual desarrollados o al equipo de propiedad privada.
- g) El acceso a equipo de propiedad privada (para verificar la seguridad de la máquina o durante una investigación), el cual puede estar prohibido por la ley.

- h) Los acuerdos sobre licencias de software que permitan que la organización sea responsable de la licencia para software de clientes en estaciones de trabajo de propiedad privada de los empleados, contratistas o usuarios de terceras partes.
- i) Protección antivirus y requisitos de barreras contra fuego (firewall).

Las directrices y disposiciones a considerar deberían incluir las siguientes:

- a) Disposición de equipo adecuado y medios de almacenamiento para las actividades de trabajo remoto, en las que no se permite el uso de equipo de propiedad privada que no esté bajo el control de la organización.
- b) Definición del trabajo que se permite realizar, las horas laborables, la confidencialidad de la información que se conserva y los sistemas y servicios internos para los cuales el trabajador tiene acceso autorizado.
- c) Disposición de equipo de comunicación apropiado, incluyendo los métodos para asegurar el acceso remoto.
- d) Seguridad física.
- e) Reglas y directrices sobre el acceso de familiares y visitantes al equipo y a la información.
- f) Disposición de soporte y mantenimiento de hardware y software.
- g) Disposición de pólizas de seguros.
- h) Procedimientos para el respaldo y la continuidad del negocio.
- i) Auditoría y monitoreo de la seguridad.
- j) Revocación de autoridad y derechos de acceso, y la devolución del equipo al finalizar las actividades de trabajo remoto.

## **Información adicional**

En el trabajo remoto se emplean tecnologías de comunicaciones que le permiten al personal realizar trabajo remoto desde un lugar fijo fuera de su organización.

### **2.2.7 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN**

#### **2.2.7.1 REQUISITOS DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN**

Garantizar que la seguridad es parte integral de los sistemas de información.

Los sistemas de información incluyen sistemas operativos, infraestructura, aplicaciones del negocio, productos de vitrina, servicios y aplicaciones desarrolladas para usuarios. El diseño y la implementación del sistema de información que da soporte a los procesos del negocio pueden ser cruciales para la seguridad. Se deberían identificar y acordar los requisitos de la seguridad antes del desarrollo y / o la implementación de los sistemas de información.

Todos los requisitos de la seguridad se deberían identificar en la fase de requisitos de un proyecto y se deberían justificar, acordar y documentar como parte de todo el caso del negocio para un sistema de información.

##### **2.2.7.1.1 ANÁLISIS Y ESPECIFICACIÓN DE LOS REQUISITOS DE LA SEGURIDAD**

#### **Control**

Las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras a los sistemas existentes deberían especificar los requisitos para los controles de la seguridad.

## **Guía de implementación**

En las especificaciones para los requisitos de control se deberían considerar los controles automatizados que se han de incorporar en el sistema de información y la necesidad de controles manuales de apoyo. Se deberían aplicar consideraciones similares al evaluar los paquetes de software, desarrollados o adquiridos, para las aplicaciones del negocio.

Los requisitos de la seguridad y los controles deberían reflejar el valor para el negocio de los activos de información involucrados y el daño potencial para el negocio que se puede presentar debido a falla o ausencia de la seguridad.

Los requisitos del sistema para la seguridad de la información y los procesos para implementarla se deberían integrar en las fases iniciales de los proyectos del sistema de información. Los controles introducidos en la etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación.

Si se adquieren productos, se debería seguir un proceso formal de adquisición y prueba.

Los contratos con el proveedor deberían abordar los requisitos de la seguridad identificados.

Cuando la funcionalidad de la seguridad de un producto determinado no satisface el requisito específico, entonces es conveniente considerar los controles de los riesgos, introducidos y asociados, antes de adquirir el producto.

Cuando se proporciona funcionalidad adicional y ello causa un riesgo de la seguridad, tal funcionalidad se debería inhabilitar o se debería revisar la estructura del control propuesto para determinar si se puede obtener ventaja de la funcionalidad mejorada disponible.

## **Información adicional**

Si se considera apropiado, por ejemplo por razones de costos, la dirección podría utilizar productos certificados y evaluados independientemente.



## **2.2.7.2 PROCESAMIENTO CORRECTO EN LAS APLICACIONES**

Evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones.

Se deberían diseñar controles apropiados en las aplicaciones, incluyendo las aplicaciones desarrolladas por el usuario para garantizar el procesamiento correcto. Estos controles deberían incluir la validación de los datos de entrada, del procesamiento interno y de los datos de salida.

Se pueden necesitar controles adicionales para los sistemas que procesan o tienen impacto en la información sensible, de valor o crítica. Dichos controles se deberían determinar con base en los requisitos de la seguridad y en una evaluación de riesgos.

### **2.2.7.2.1 VALIDACIÓN DE LOS DATOS DE ENTRADA**

#### **Control**

Se deberían validar los datos de entrada a las aplicaciones para asegurar que dichos datos son correctos y apropiados.

#### **Guía de implementación**

Es recomendable realizar verificaciones de las entradas de las transacciones del negocio, de los datos permanentes (por ejemplo, nombres y direcciones, límites de crédito, números de referencia del cliente) y de las tablas de parámetros (por ejemplo, precios de venta, tasas de conversión de divisas, tasas de impuestos). Se recomienda tomar en consideración las siguientes directrices:

- a) Verificaciones de entradas duales u otras entradas, tales como verificación de fronteras o campos limitantes para especificar los rangos de los datos de entrada, con el fin de detectar los siguientes errores:
  - a. Valores fuera de rango.
  - b. Caracteres no válidos en los campos de datos.

- c. Datos incompletos o ausentes.
  - d. Exceso en los límites superiores e inferiores del volumen de datos.
  - e. Datos de controles inconsistentes o no autorizados.
- 
- b) Revisión periódica del contenido de los campos clave o de los archivos de datos para confirmar su validez e integridad.
  - c) Inspección de los documentos de entrada impresos para determinar cambios no autorizados (todos los cambios en los datos de entrada deben estar autorizados).
  - d) Procedimientos de respuesta ante errores de validación.
  - e) Procedimientos para probar la credibilidad de los datos de entrada.
  - f) Definición de responsabilidades para todo el personal que participa en el proceso de entrada de datos.
  - g) Creación de un registro de las actividades implicadas en el proceso de entrada de datos.

### **Información adicional**

Se recomienda la inspección y la validación automática de los datos de entrada, cuando se puedan aplicar, para reducir el riesgo de errores y evitar ataques normales, incluyendo desbordamiento de búfer o inyección de códigos.

### **2.2.7.2.2 CONTROL DE PROCESAMIENTO INTERNO**

#### **Control**

Se deberían incorporar verificaciones de validación en las aplicaciones para detectar cualquier daño o pérdida de la información por errores de procesamiento o actos deliberados.

## Guía de implementación

El diseño y la implementación de las aplicaciones deberían garantizar que se minimizan los riesgos de falla en el procesamiento, los cuales originan pérdida de la integridad. Las áreas específicas que se han de considerar incluyen:

- a) Utilización de las funciones agregar, modificar y borrar para implementar los cambios en los datos.
- b) Procedimientos para evitar que los programas se ejecuten en orden erróneo o su ejecución después de una falla previa del procesamiento.
- c) Utilización de programas adecuados para la recuperación después de fallas con el fin de garantizar el procesamiento correcto de los datos.
- d) Protección contra ataques empleando desbordamiento / exceso en el búfer.

Se deberían elaborar listas de verificación adecuadas, documentar las actividades y mantener seguros los resultados. Los siguientes son algunos ejemplos de verificaciones que se pueden incorporar:

- a) Controles de sesión o de lotes, para conciliar los balances de archivos de datos después de actualizar las transacciones.
- b) Controles de balance, para verificar los balances de apertura frente a los balances de cierre previos, tales como:
  - a. Controles para cada ejecución.
  - b. Totales de actualizaciones de archivos.
  - c. Controles programa a programa.
- c) Validación de los datos de entrada generados por el sistema.
- d) Verificaciones de la integridad, la autenticidad o cualquier otra característica de seguridad de los datos o del software descargado o actualizado entre el computador central y el remoto.

- e) Totales de verificación (hash) de registros y archivos.
- f) Verificaciones para garantizar que los programas de aplicación se ejecutan en el momento correcto.
- g) Verificaciones para garantizar que los programas se ejecutan en el orden correcto y finalizan en caso de falla, y que el procesamiento posterior se detiene hasta resolver el problema.
- h) Creación de un registro de las actividades implicadas en el procesamiento.

### **Información adicional**

Los datos que se han ingresado correctamente se pueden corromper por errores de software, errores de procesamiento o a través de actos deliberados. Las verificaciones de validación requeridas dependerán de la naturaleza de la aplicación y del impacto de la corrupción de los datos en el negocio.

### **2.2.7.3 INTEGRIDAD DEL MENSAJE**

#### **Control**

Se deberían identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados.

#### **Guía de implementación**

Se debería realizar una evaluación de los riesgos de la seguridad para determinar si se requiere integridad del mensaje y para identificar el método más apropiado de implementación.

### **Información adicional**

Se pueden usar las técnicas criptográficas como un medio apropiado para implementar la autenticación del mensaje.

### **2.2.7.3.1 VALIDACIÓN DE LOS DATOS DE SALIDA**

#### **Control**

Se deberían validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias.

#### **Guía de implementación**

La validación de los datos de salida puede incluir:

- a) Verificaciones de la verosimilitud para probar si los datos de salida son razonables.
- b) Cuentas de control de conciliación para asegurar el procesamiento de todos los datos.
- c) Suministro de información suficiente para que un lector o un sistema de procesamiento posterior determine la exactitud, totalidad, precisión y clasificación de la información.
- d) Procedimientos para responder las pruebas de validación de salidas.
- e) Definición de las responsabilidades de todo el personal que participa en el proceso de la salida de datos.
- f) Creación de un registro de las actividades del proceso de validación de la salida de datos.

#### **Información adicional**

Comúnmente, los sistemas y las aplicaciones se construyen asumiendo que al realizar la validación, la verificación y las pruebas adecuadas, la salida siempre será correcta. Sin embargo, esta suposición no siempre es válida, es decir, los sistemas que se han sometido a prueba aún pueden producir salidas incorrectas en algunas circunstancias.

## **2.2.7.4 CONTROLES CRIPTOGRÁFICOS**

Proteger la confidencialidad, autenticidad o integridad de la información, por medios criptográficos.

Se debería desarrollar una política sobre el uso de los controles criptográficos y establecer una gestión de claves para dar soporte al empleo de técnicas criptográficas.

### **2.2.7.4.1 POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS**

#### **Control**

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

#### **Guía de implementación**

Se recomienda tomar en consideración los siguientes aspectos al desarrollar una política criptográfica:

- a) El enfoque de la dirección hacia el uso de controles criptográficos en toda la organización, incluyendo los principios generales bajo los cuales se debería proteger la información del negocio.
- b) Con base en una evaluación de riesgos, se debería identificar el nivel requerido de protección teniendo en cuenta tipo, fortaleza y calidad del algoritmo de encriptación requerido.
- c) Uso de encriptación para la protección de la información sensible transportada por medios móviles o removibles, por dispositivos o a través de las líneas de comunicación.
- d) Enfoque para la gestión de claves, incluyendo los métodos para tratar la protección de las claves criptográficas y la recuperación de información encriptada en caso de pérdida, amenaza o daño de las claves.

- e) Funciones y responsabilidades, por ejemplo, quién es responsable de:
  - a. La implementación de la política.
  - b. La gestión de claves, incluyendo su generación.
- f) Normas que se han de adoptar para la implementación eficaz en toda la organización (qué solución se usa para cuáles procesos del negocio).
- g) Impacto de la utilización de información encriptada sobre los controles que depende de la inspección del contenido (por ejemplo, detección de virus).

Cuando se implementa la política de encriptación de la organización, es conveniente tener en mente los reglamentos y las restricciones nacionales que se pueden aplicar al uso de técnicas criptográficas en diferentes partes del mundo y los aspectos del flujo trans-fronterizo de información encriptada.

Los controles criptográficos se pueden utilizar para lograr diferentes objetivos de la seguridad, por ejemplo:

- a) Confidencialidad: uso de encriptación de la información para proteger información sensible o crítica, bien sea almacenada o transmitida.
- b) Integridad/autenticidad: uso de firmas digitales o códigos de autenticación de mensajes para proteger la autenticidad e integridad de información sensible o crítica transmitida o almacenada.
- c) No – repudio: uso de técnicas criptográficas para obtener prueba de la ocurrencia o no ocurrencia de un evento o acción.

### **Información adicional**

La decisión sobre la idoneidad de la solución criptográfica debería formar parte del proceso más amplio de evaluación de riesgos y selección de controles. Esta evaluación se puede usar para determinar si un control criptográfico es adecuado, el tipo de control que se debería aplicar y para qué propósito y cuál proceso del negocio.

La política sobre el empleo de controles criptográficos es necesaria para maximizar los beneficios y minimizar los riesgos de usar las técnicas criptográficas, y para evitar el uso incorrecto o inapropiado. Cuando se utilizan firmas digitales, se recomienda considerar toda la legislación pertinente, en particular la legislación que describe las condiciones bajo las cuales la firma digital es legalmente obligatoria.

Es conveniente buscar asesoría especializada para identificar el nivel apropiado de protección y definir las especificaciones adecuadas que suministrarán la protección requerida y el soporte a la implementación de un sistema seguro de gestión de claves.

#### **2.2.7.4.2 GESTIÓN DE CLAVES**

##### **Control**

Se debería establecer la gestión de claves para apoyar el uso de técnicas criptográficas en la organización.

##### **Guía de implementación**

Todas las claves criptográficas deberían tener protección contra modificación, pérdida y destrucción. Además, las claves privadas y secretas necesitan protección contra divulgación no autorizada. El equipo usado para generar, almacenar y archivar las claves debería estar protegido por medios físicos.

Un sistema de gestión de claves se debería basar en un conjunto acordado de normas, procedimientos y método seguros para:

- a) Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.
- b) Generar y obtener certificados de claves públicas.
- c) Distribuir claves a los usuarios previstos, incluyendo la forma de activar y recibir las claves.
- d) Almacenar las claves, incluyendo la forma en que los usuarios autorizados tendrán acceso a ellas.



- e) Cambiar o actualizar las claves incluyendo reglas sobre cuándo cambiarlas y cómo hacerlo.
- f) Tratar las claves perdidas.
- g) Revocar las claves, incluyendo la forma de retirarlas o desactivarlas, por ejemplo, cuando las claves se han puesto en peligro o cuando un usuario se retira de la organización (en cuyo caso las claves también se deberían archivar).
- h) Recuperar claves pérdidas o corruptas como parte de la gestión de continuidad del negocio. por ejemplo, para la recuperación de información encriptada.
- i) Archivar claves, por ejemplo para la información archivada o con copia de respaldo.
- j) Destrucción de claves.
- k) Registro y auditoría de las actividades relacionadas con la gestión de claves.

Para reducir la probabilidad de poner en peligro, activar o desactivar se deberían definir fechas para las claves de modo que sólo se puedan utilizar durante un periodo de tiempo limitado.

Este período dependería de las circunstancias en las cuales se usa el control criptográfico y del riesgo percibido.

Además de las claves privadas y secretas con gestión segura, también se debería pensar en la autenticidad de las claves públicas. Este proceso de autenticación se puede hacer con certificados de claves públicas que normalmente son emitidos por una autoridad de certificación, la cual debe ser una organización reconocida con controles y procedimientos idóneos establecidos para proporcionar el grado requerido de confianza.

El contenido de los acuerdos o contratos de servicios con proveedores externos de servicios criptográficos, por ejemplo con una autoridad de certificación, deberían comprender aspectos de responsabilidad, confiabilidad de los servicios y tiempos de respuesta para la prestación de los servicios.

## **Información adicional**

La gestión de las claves criptográficas es esencial para el uso eficaz de las técnicas criptográficas. Los dos tipos de técnicas criptográficas son:

- a) Técnicas de clave secreta, en donde dos o más partes comparten la misma clave y ésta se usa tanto para encriptar como des encriptar información. esta clave debe mantenerse secreta puesto que cualquiera que tenga acceso a ella puede descifrar toda la información encriptada con dicha clave, o introducir información no autorizada con esa clave.
  
- b) Técnicas de clave pública, en donde cada usuario tiene un par de claves, una clave pública (que se puede revelar a cualquiera) y una clave privada (que se debe mantener en secreto). las técnicas de clave pública se pueden usar para la encriptación y para producir firmas digitales.

Existe una amenaza de falsificar una firma digital reemplazando la clave pública del usuario. Este problema se puede tratar usando un certificado de clave pública.

Las técnicas criptográficas también se pueden usar para proteger las claves criptográficas. Es necesario que en los procedimientos se considere el manejo de solicitudes legales para acceder a las claves criptográficas, por ejemplo, puede ser necesario poner a disposición la información encriptada en un formato sin encriptación como evidencia en caso de un juicio.

### **2.2.7.5 SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA**

Garantizar la seguridad de los archivos del sistema.

Los accesos a los archivos del sistema y al código fuente del programa deberían estar protegidos, y los proyectos de tecnología de la información y las actividades de soporte se deberían efectuar de forma segura. Se debería tener cuidado para evitar la exposición de datos sensibles en los entornos de prueba.

### **2.2.7.5.1 CONTROL DEL SOFTWARE OPERATIVO**

#### **Control**

Se deberían establecer procedimientos para controlar la instalación de software en los sistemas operativos.

#### **Guía de implementación**

Para minimizar los riesgos de corrupción de los sistemas operativos, se deberían tener en cuenta las siguientes directrices para controlar los cambios:

- a) La actualización del software operativo, las aplicaciones y las bibliotecas de los programas sólo deberían ser realizadas por administradores capacitados y con la debida autorización de la dirección.
- b) Los sistemas operativos únicamente deberían contener códigos ejecutables aprobados y no códigos en desarrollo ni compiladores.
- c) El software de las aplicaciones y del sistema operativo sólo se deberían implementar después del ensayo exhaustivo y exitoso. los ensayos deberían incluir pruebas sobre capacidad de uso, seguridad, efectos en otros sistemas y facilidad para el usuario, igualmente se deberían efectuar en sistemas separados. se debería garantizar que todas las bibliotecas fuente del programa correspondiente estén actualizadas.
- d) Se debería usar un sistema de control de configuración para mantener el control el software implementado, así como de la documentación del sistema.
- e) Es conveniente implantar una política de estrategia de restauración al estado anterior antes de implementar los cambios.
- f) Se debería conservar un registro para auditoría de todas las actualizaciones de las bibliotecas de los programas operativos.
- g) Es conveniente conservar las versiones anteriores del software de aplicación como medida de contingencia.

- h) Las versiones antiguas del software se deberían archivar junto con toda la información requerida y los parámetros, procedimientos, detalles de configuración y software de soporte, en la medida en que los datos se retengan en archivo.

El software suministrado por el vendedor utilizado en los sistemas operativos se debería mantener en el nivel con soporte del proveedor. Con el tiempo, los vendedores de software dejarán de dar soporte a las versiones antiguas del software. La organización debería considerar los riesgos de depender de software sin soporte.

En toda decisión para mejorar a una nueva versión se debería contar con los requisitos del negocio para el cambio, y la seguridad de la nueva versión, es decir, la introducción de nueva funcionalidad en el sistema o la cantidad y gravedad de los problemas de seguridad que afectan a esta versión. Los parches de software se deberían aplicar cuando pueden ayudar a eliminar o reducir las debilidades de la seguridad.

El acceso físico o lógico únicamente se debería dar a los proveedores para propósitos de soporte, cuando sea necesario, y con aprobación de la dirección. Las actividades del proveedor se deberían monitorear.

El software del computador puede depender de software y módulos suministrados externamente, lo cual se debería monitorear y controlar para evitar cambios no autorizados que puedan introducir debilidades de seguridad.

### **Información adicional**

Los sistemas operativos únicamente se deberían mejorar cuando existe una necesidad para hacerlo, por ejemplo, si la versión actual del sistema operativo ya no da soporte a los requerimientos del negocio. Las mejoras no deberían tener lugar sólo porque esté disponible una nueva versión del sistema operativo. Las versiones nuevas del sistema operativo pueden ser menos seguras, menos estables, y menos entendidas que los sistemas actuales.

## **2.2.7.5.2 PROTECCIÓN DE LOS DATOS DE PRUEBA DEL SISTEMA**

### **Control**

Los datos de prueba deberían seleccionarse cuidadosamente, así como protegerse y controlarse.

### **Guía de implementación**

Se debería evitar el uso de bases de datos operativos que contienen información personal o cualquier otra información sensible con propósitos de prueba. Si se utiliza información personal o de otra forma sensible para propósitos de prueba, todos los detalles y el contenido sensible se deberían retirar o modificar antes del uso para evitar el reconocimiento.

Las siguientes directrices se deberían aplicar para proteger los datos operativos cuando se emplean con propósitos de prueba:

- a) Los procedimientos de control del acceso que se aplican a los sistemas de aplicación operativos también se deberían aplicar a los sistemas de aplicación de pruebas.
- b) Debería existir autorización separada cada vez que se copia la información operativa en un sistema de aplicación de prueba.
- c) La información operativa se debería borrar del sistema de aplicación de prueba inmediatamente después de terminar la prueba.
- d) El copiado y utilización de la información operativa se debería registrar para brindar un rastro para auditoría.

### **Información adicional**

La prueba del sistema y de aceptación usualmente exige volúmenes sustanciales de datos de prueba que sean lo más cercanos posible a los datos operativos.

### **2.2.7.5.3 CONTROL DE ACCESO AL CÓDIGO FUENTE DE LOS PROGRAMAS**

#### **Control**

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

#### **Guía de implementación**

El acceso al código fuente de programas y a los elementos asociados (como diseños, especificaciones, planes de verificación y planes de validación) se debería controlar estrictamente para evitar la introducción de funcionalidad no autorizada y evitar los cambios involuntarios.

Para el código fuente de programas esto se puede lograr con el almacenamiento central controlado de dicho código, preferiblemente en las bibliotecas fuente de programas. Las siguientes directrices se deberían considerar para controlar el acceso a tales bibliotecas fuente de programas, con el objeto de reducir el potencial de corrupción de los programas del computador:

- a) Cuando sea posible, las bibliotecas fuente de programas no se deberían mantener en los sistemas operativos.
- b) El código fuente de programas y las bibliotecas fuente de programas se deberían gestionar de acuerdo con los procedimientos establecidos.
- c) El personal de soporte debería tener acceso restringido a las bibliotecas fuente de programas.
- d) La actualización de las bibliotecas fuente de programas y de los elementos asociados, así como la emisión de fuentes de programa a los programadores, solamente se debería efectuar después de recibir la autorización apropiada.
- e) Los listados de programas se deberían mantener en un entorno seguro.
- f) Se debería conservar un registro para auditoría de todos los accesos a las bibliotecas fuente de programas.

- g) El mantenimiento y el copiado de las bibliotecas fuente de programas deberían estar sujetos a un procedimiento estricto de control de cambios.

### **Información adicional**

El código fuente de programas es un código escrito por los programadores, el cual está compilado (y enlazado) para crear ejecutables. Algunos lenguajes de programación no distinguen formalmente entre el código fuente y los ejecutables ya que estos últimos se crean en el momento en que se activan.

### **2.2.7.6 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE**

Mantener la seguridad del software y de la información del sistema de aplicaciones.

Los entornos de soporte y de desarrollo deberían estar estrictamente controlados.

Los directores responsables de los sistemas de aplicación también deberían ser responsables de la seguridad del entorno del proyecto o del soporte. Ellos deberían garantizar que todos los cambios propuestos en el sistema se revisan para comprobar que no ponen en peligro la seguridad del sistema ni del entorno operativo.

#### **2.2.7.6.1 PROCEDIMIENTOS DE CONTROL DE CAMBIOS**

##### **Control**

Se debería controlar la implementación de cambios utilizando procedimientos formales de control de cambios.

##### **Guía de implementación**

Los procedimientos formales de control de cambios se deberían documentar y hacer cumplir para minimizar la corrupción de los sistemas de información. La introducción de sistemas nuevos y de cambios importantes en los sistemas existentes debería seguir un proceso formal de documentación, especificación, prueba, control de calidad e implementación con gestión.

Este proceso debería incluir una evaluación de riesgos, análisis de los impactos de los cambios y especificación de los controles de seguridad necesarios. Este proceso también debería garantizar que la seguridad y los procesos de control existentes no se ponen en peligro, que se da acceso a los programadores de soporte sólo a aquellas partes del sistema necesarias para su trabajo y que existe acuerdo y aprobación formal para cualquier cambio.

Siempre que sea factible, los procedimientos de control de cambios operativos y de aplicación se deberían integrar. Los procedimientos de control de cambios deberían incluir:

- a) El mantenimiento de un registro de los niveles acordados de autorización.
- b) La garantía de que los cambios son realizados por los usuarios autorizados.
- c) La revisión de los controles y de los procedimientos de integridad para asegurar que no se pondrán en peligro debido a los cambios.
- d) La identificación de todo el software, la información, las entidades de bases de datos y del hardware que requieran mejora.
- e) La obtención de la aprobación formal de las propuestas detalladas antes de iniciar el trabajo.
- f) La garantía de que los usuarios autorizados aceptan los cambios antes de la implementación.
- g) La garantía de que la documentación del sistema está actualizada al finalizar cada cambio y que la documentación antigua se archiva o elimina.
- h) El mantenimiento de una versión de control para todas las actualizaciones de software.
- i) El mantenimiento de un rastro para auditoría de todos los cambios solicitados.
- j) La garantía de que la documentación operativa y los procedimientos de usuario se cambian en función de la necesidad con el objeto de mantener su idoneidad.



- k) La garantía de que la implementación de los cambios tiene lugar en el momento oportuno y no perturba los procesos del negocio involucrados.

### **Información adicional**

El cambio del software puede tener impacto en el entorno operativo.

Una buena práctica incluye la prueba del software nuevo en un entorno separado tanto del entorno de producción como del de desarrollo. Esto proporciona medios para controlar el software nuevo y facilitar la protección adicional de la información operativa que se usa con propósitos de prueba. Se deberían incluir parches, paquetes de servicio y otras actualizaciones. Las actualizaciones automáticas no se deberían utilizar en sistemas críticos ya que algunas de ellas pueden causar fallas de las aplicaciones críticas.

### **2.2.7.6.2 REVISIÓN TÉCNICA DE LAS APLICACIONES DESPUÉS DE LOS CAMBIOS EN EL SISTEMA OPERATIVO**

#### **Control**

Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deberían revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización.

#### **Guía de implementación**

Este proceso debería comprender los siguientes aspectos:

- a) Revisión de los procedimientos de integridad y control de la aplicación para asegurarse de que no se han puesto en peligro debido a los cambios en el sistema operativo.
- b) Garantía de que el plan y el presupuesto de soporte anual cubrirán las revisiones y pruebas del sistema que resulten de cambios en el sistema operativo.

- c) Garantía de la notificación oportuna sobre los cambios en el sistema operativo para permitir la realización de las pruebas y las revisiones apropiadas antes de la implementación.
- d) Garantía de que se hacen cambios en los planes de continuidad del negocio.

Un grupo o un individuo específico debería ser responsable de monitorear las vulnerabilidades y las nuevas versiones de parches y arreglos (fixes) del distribuidor.

### **2.2.7.6.3 RESTRICCIONES EN LOS CAMBIOS A LOS PAQUETES DE SOFTWARE**

#### **Control**

Se debería desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.

#### **Guía de implementación**

En la medida de lo posible y viable, los paquetes de software suministrados por el vendedor se deberían usar sin modificaciones. Cuando sea necesario modificar un paquete de software, se deberían tener en cuenta los siguientes puntos:

- a) El riesgo de que los procesos de integridad y de control incorporados se vean comprometidos.
- b) Si es necesario obtener el consentimiento del vendedor.
- c) La posibilidad de obtener los cambios requeridos del vendedor como un programa estándar de actualizaciones.
- d) El impacto, si la organización se hace responsable del mantenimiento futuro del software como resultado de los cambios.

Si los cambios son necesarios, el software original se debería conservar y los cambios se deberían aplicar a una copia claramente identificada.

Se debería implementar un proceso de gestión de las actualizaciones del software para asegurarse de que los parches más actualizados aprobados y las actualizaciones de las aplicaciones están instalados en todo el software autorizado. Todos los cambios se deberían probar y documentar en su totalidad de manera que se puedan volver a aplicar, si es necesario, para mejoras futuras del software.

Si así se requiere, las modificaciones se deberían probar y validar por un organismo de evaluación independiente.

#### **2.2.7.6.4 FUGA DE INFORMACIÓN**

##### **Control**

Se deberían evitar las oportunidades para que se produzca fuga de información.

##### **Guía de implementación**

Se deberían considerar los siguientes aspectos para limitar el riesgo de fuga de información, por ejemplo, mediante el uso y explotación de los canales encubiertos:

- a) Exploración de los medios y comunicaciones de salida para determinar la información oculta.
- b) Comportamiento de las comunicaciones y del sistema de modulación y enmascaramiento para reducir la probabilidad de que una tercera parte pueda deducir información a partir de tal comportamiento.
- c) Utilización de sistemas y software que se consideran con integridad alta, por ejemplo usar productos evaluados.
- d) Monitoreo regular de las actividades del personal y del sistema, cuando está permitido por la legislación o los reglamentos existentes.
- e) Monitoreo del uso de los recursos en los sistemas de computador.

## **Información adicional**

Los canales encubiertos son vías que no están destinadas para conducir flujos de información, pero que, sin embargo, pueden existir en un sistema o una red. Por ejemplo, los bits de manipulación en los paquetes de protocolo de comunicaciones se podrían usar como un método oculto de señalización.

Debido a su naturaleza, evitar la existencia de todos los posibles canales encubiertos sería difícil, si no imposible. No obstante, la explotación de tales canales se realiza con frecuencia a través de códigos troyanos.

Por lo tanto, tomar medidas para proteger contra códigos troyanos reduce el riesgo de explotación de los canales encubiertos.

La prevención del acceso no autorizado a la red, así como las políticas y los procedimientos para desalentar el uso inadecuado de los servicios de información por parte del personal facilitarán la protección contra canales encubiertos.

### **2.2.7.6.5 DESARROLLO DE SOFTWARE CONTRATADO EXTERNAMENTE**

#### **Control**

La organización debería supervisar y monitorear el desarrollo de software contratado externamente.

#### **Guía de implementación**

Cuando el desarrollo del software se contrata externamente, se recomienda tener en cuenta los siguientes puntos:

- a) Acuerdos sobre licencias, propiedad de los códigos y derechos de propiedad intelectual.
- b) Certificación de la calidad y exactitud del trabajo realizado.
- c) Convenios de fideicomiso en caso de falla de la tercera parte.

- d) Derechos de acceso para auditar la calidad y exactitud del trabajo realizado.
- e) Requisitos contractuales para la calidad y la funcionalidad de la seguridad del código.
- f) Realización de pruebas antes de la instalación para detectar códigos troyanos o maliciosos.

### **2.2.7.7 GESTIÓN DE LA VULNERABILIDAD TÉCNICA**

Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.

La gestión de la vulnerabilidad técnica se debería implementar de forma eficaz, sistemática y repetible con toma de mediciones para confirmar su eficacia. Estas consideraciones deberían incluir a los sistemas operativos y otras aplicaciones en uso.

#### **2.2.7.7.1 CONTROL DE LAS VULNERABILIDADES TÉCNICAS**

##### **Control**

Se debería obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.

##### **Guía de implementación**

Un inventario completo y actual de los activos es un prerrequisito para la gestión eficaz de la vulnerabilidad técnica. La información específica necesaria para dar soporte a la gestión de la vulnerabilidad técnica incluye los siguientes datos: vendedor del software, números de versión, estado actual de despliegue (por ejemplo qué software está instalado en cuál sistema) y las personas de la organización responsables del software.

Es conveniente tomar la acción oportuna y apropiada en respuesta a la identificación de vulnerabilidades técnicas potenciales. Se recomienda tener en cuenta las siguientes directrices para establecer un proceso de gestión eficaz de las vulnerabilidades técnicas:

- a) La organización debería definir e instaurar las funciones y responsabilidades asociadas con la gestión de la vulnerabilidad técnica, incluyendo el monitoreo de la vulnerabilidad, la evaluación de riesgos de la vulnerabilidad, el uso de parches, el rastreo de activos y todas las responsabilidades de coordinación requeridas.
- b) Es conveniente identificar los recursos de información que se van a utilizar para identificar las vulnerabilidades técnicas pertinentes y para mantener la concientización sobre ellas para el software y otra tecnología, estos recursos de información se deberían actualizar en función de los cambios en el inventario o cuando se encuentran recursos nuevos o útiles.
- c) Se debería definir una línea de tiempo para reaccionar ante la notificación de vulnerabilidades técnicas potenciales pertinentes.
- d) Una vez se ha identificado una vulnerabilidad potencial, la organización debería identificar los riesgos asociados y las acciones que se han de tomar. tales acciones podrían involucrar el uso de parches en los sistemas vulnerables y / o la aplicación de otros controles.
- e) Dependiendo de la urgencia con la que es necesario tratar la vulnerabilidad técnica, la acción a tomar se debería ejecutar de acuerdo con los controles relacionados con la gestión de cambios o siguiendo los procedimientos de respuesta ante incidentes de seguridad de la información.
- f) Si está disponible un parche, se deberían evaluar los riesgos asociados con su instalación (los riesgos impuestos por la vulnerabilidad se deberían comparar con los riesgos de instalar el parche).
- g) Es conveniente probar y evaluar los parches antes de su instalación para garantizar que son eficaces y no producen efectos secundarios intolerables. si no hay parche disponible, se recomienda considerar otros controles:
  - a. Apagar los servicios o capacidades relacionadas con la vulnerabilidad.

- b. Adaptar o agregar controles de acceso, por ejemplo, barreras de fuego (firewalls), en las fronteras de la red.
  - c. Aumentar el monitoreo para detectar o prevenir los ataques reales.
  - d. Crear conciencia sobre la vulnerabilidad.
- 
- h) Se debería conservar un registro para auditoría para todos los procedimientos efectuados.
  - i) El proceso de gestión de la vulnerabilidad técnica se debería monitorear y evaluar a intervalos regulares para garantizar su eficacia y eficiencia.
  - j) Se deberían tratar primero los sistemas con alto riesgo.

### **Información adicional**

El funcionamiento correcto del proceso de gestión de la vulnerabilidad técnica es crítico para muchas organizaciones y por ello se debería monitorear con regularidad. Es esencial un inventario exacto para garantizar la identificación de vulnerabilidades técnicas potenciales y pertinentes.

La gestión de la vulnerabilidad técnica se puede ver como una sub-función de la gestión de cambios y como tal puede tomar ventaja de los procesos y procedimientos de gestión de cambios.

Los vendedores, con frecuencia, están bajo gran presión para sacar a la venta los parches tan pronto sea posible. Por lo tanto, es posible que un parche no trate el problema adecuadamente y tenga efectos colaterales negativos. En algunos casos, desinstalar un parche puede no ser tan fácil una vez que se ha aplicado.

Si no es posible someter los parches a las pruebas adecuadas, por ejemplo, debido a los costos o a la falta de recursos, se puede pensar en retrasar la aplicación del parche para valorar los riesgos asociados, basados en la experiencia reportada por otros usuarios.

## **2.2.8 GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN**

### **2.2.8.1 REPORTE SOBRE LOS EVENTOS Y LAS DEBILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN**

Asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.

Es conveniente establecer el reporte formal del evento y los procedimientos de escalada.

Todos los empleados, contratistas y usuarios de tercera parte deberían tener conciencia sobre los procedimientos para el reporte de los diferentes tipos de evento y las debilidades que puedan tener impacto en la seguridad de los activos de la organización. Se les debería exigir que reporten todos los eventos de seguridad de la información y las debilidades tan pronto sea posible al punto de contacto designado.

#### **2.2.8.1.1 REPORTE SOBRE LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN**

##### **Control**

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

##### **Guía de implementación**

Se debería instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente que establezca la acción que se ha de tomar al recibir el reporte sobre un evento de seguridad de la información. Se debería establecer un punto de contacto para el reporte de los eventos de seguridad de la información. Es conveniente garantizar que este punto de contacto se conoce en toda la organización, siempre está disponible y puede suministrar respuesta oportuna y adecuada.



Todos los empleados, contratistas y usuarios de tercera parte deberían tener conciencia de su responsabilidad para reportar todos los eventos de seguridad de la información lo más pronto posible. Deberían conocer el procedimiento para reportar los eventos de seguridad de la información y el punto de contacto.

Los procedimientos de reporte deberían incluir los siguientes aspectos:

- a) Procesos adecuados de retroalimentación para garantizar que aquellos que reportan los eventos de seguridad de la información reciben notificación de los resultados después de que se ha tratado y solucionado el problema.
- b) Formatos para el reporte de los eventos de seguridad de la información para contener la acción de reporte y ayudar a que la persona que hace el reporte recuerde todas las acciones necesarias en caso de un evento de seguridad de la información.
- c) El comportamiento correcto en caso de un evento de seguridad de la información, es decir:
  - a. Tomar nota inmediatamente sobre los detalles importantes (por ejemplo, tipo de incumplimiento o violación, disfunción que se presenta, mensajes en la pantalla, comportamiento extraño).
  - b. No ejecutar ninguna acción propia sino reportarla inmediatamente al punto de contacto.
- d) Referencia a un proceso disciplinario formal establecido para tratar a los empleados, contratistas o usuarios de tercera parte que cometieron la violación de la seguridad.

En entornos de alto riesgo, se puede suministrar una alarma de coacción<sup>2</sup> a través de la cual una persona bajo coacción pueda indicar tales problemas. Los procedimientos para responder a las alarmas de coacción deberían reflejar la situación de alto riesgo que indican tales alarmas.

### **Información adicional**

---

<sup>2</sup> Una alarma de coacción es un método para indicar secretamente que tiene lugar una acción "bajo coacción".

Los siguientes son ejemplos de eventos e incidentes de seguridad.

- a) Pérdida del servicio, del equipo o de las prestaciones.
- b) Mal funcionamiento o sobrecargas del sistema.
- c) Errores humanos.
- d) Incumplimientos de las políticas o las directrices.
- e) Violaciones de las disposiciones de seguridad física.
- f) Cambios no controlados en el sistema.
- g) Mal funcionamiento del software o del hardware,
- h) Violaciones del acceso.

Con el debido cuidado de los aspectos de confidencialidad, los incidentes de seguridad de la información se pueden usar en la formación sobre toma de conciencia de los usuarios como ejemplos de lo que podría pasar, cómo responder a tales incidentes y cómo evitarlos en el futuro. Para poder tratar adecuadamente los eventos e incidentes de seguridad de la información podría ser necesario recolectar evidencia tan pronto sea posible después del suceso.

El mal funcionamiento u otro comportamiento anómalo del sistema puede ser un indicador de un ataque de seguridad o una violación real de la seguridad y por lo tanto siempre se debería reportar como evento de seguridad de la información.

#### **2.2.8.1.2 REPORTE SOBRE LAS DEBILIDADES EN LA SEGURIDAD**

##### **Control**

Se debería exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.

## **Guía de implementación**

Todos los empleados, contratistas y usuarios de terceras partes deberían informar sobre estos asuntos a su director o directamente a su proveedor de servicio, tan pronto sea posible para evitar los incidentes de seguridad de la información. Los mecanismos de reporte deberían ser fáciles, accesibles y disponibles. Se les debería informar a ellos que, en ninguna circunstancia, deberían intentar probar una debilidad sospechada.

### **Información adicional**

A todos los empleados, contratistas y usuarios de tercera parte se les debería aconsejar no intentar probar debilidades sospechadas en la seguridad. El ensayo de las debilidades se podría interpretar como un posible uso inadecuado del sistema y también podría causar daño al sistema o servicio de información que origine una responsabilidad legal por la realización individual del ensayo.

#### **2.2.8.2 GESTIÓN DE LOS INCIDENTES Y LAS MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN**

Objetivo: asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.

Es conveniente establecer las responsabilidades y los procedimientos para manejar los eventos y debilidades de la seguridad de la información de manera eficaz una vez se han reportado. Se debería aplicar un proceso de mejora continua a la respuesta para monitorear, evaluar y gestionar en su totalidad los incidentes de seguridad de la información.

Cuando se requiere evidencia, ésta se debería recolectar para garantizar el cumplimiento de los requisitos legales.

## 2.2.8.2.1 RESPONSABILIDADES Y PROCEDIMIENTOS

### Control

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

### Guía de implementación

Además del reporte de los eventos y las debilidades de la seguridad de la información, el monitoreo de los sistemas, las alertas y las vulnerabilidades se debería emplear para detectar los incidentes de la seguridad de la información.

Se recomienda tener en cuenta las siguientes directrices para los procedimientos de gestión de los incidentes de seguridad de la información:

- a) Es conveniente implantar procedimientos para manejar los diferentes tipos de incidentes de seguridad de la información, incluyendo:
  - a. Fallas en el sistema de información y pérdida del servicio.
  - b. Códigos maliciosos.
  - c. Negación del servicio.
  - d. Errores producidos por datos del negocio, incompletos o inexactos.
  - e. Violaciones de la confidencialidad y la integridad.
  - f. Uso inadecuado de los sistemas de información.
- b) Además de los planes normales de contingencia, los procedimientos también deberían comprender:
  - a. El análisis y la identificación de la causa del incidente.
  - b. La contención.

- c. La planificación e implementación de la acción correctiva para evitar la recurrencia, si es necesario.
  - d. La comunicación con aquellos afectados o implicados con la recuperación después del incidente.
  - e. El reporte de la acción a la autoridad apropiada.
- c) Se deberían recolectar y asegurar las pistas para la auditoría y la evidencia similar, según sea apropiado para:
- a. El análisis de los problemas internos.
  - b. El uso de evidencia forense con respecto a la posible violación del contrato o del requisito reglamentario o en caso de juicios criminales o civiles, por ejemplo, según la legislación sobre uso inadecuado del computador o sobre protección de datos.
  - c. La negociación para la compensación proveniente de los proveedores de software y servicios.
- d) La acción para la recuperación de las violaciones de la seguridad y la corrección de las fallas del sistema debería estar cuidadosa y formalmente controlada. los procedimientos deberían garantizar que:
- a. Únicamente el personal claramente identificado y autorizado tiene acceso a los sistemas y datos activos.
  - b. Todas las acciones de emergencia están documentadas en detalle.
  - c. La acción de emergencia se reporta a la dirección y se revisa de manera ordenada.
  - d. La integridad de los sistemas y controles del negocio se confirma con retraso mínimo.

Los objetivos de la gestión de los incidentes de seguridad de la información se deberían acordar con la dirección y se debería garantizar que los responsables de esta gestión comprenden las prioridades de la organización para el manejo de los incidentes de seguridad de la información.

### **Información adicional**

Los incidentes de seguridad de la información podrían trascender las fronteras de la organización y las nacionales. Para responder a tales incidentes existe la necesidad creciente de coordinar la respuesta y compartir la información sobre estos incidentes con las organizaciones externas, según sea apropiado.

## **2.2.8.2.2 APRENDIZAJE DEBIDO A LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**

### **Control**

Deberían existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.

### **Guía de implementación**

La información que se obtiene de la evaluación de los incidentes de seguridad de la información se debería utilizar para identificar los incidentes recurrentes o de alto impacto.

### **Información adicional**

La evaluación de los incidentes de seguridad de la información puede indicar la necesidad de mejorar o agregar controles para limitar la frecuencia, el daño y el costo de futuras recurrencias, o de considerarlos en el proceso de revisión de la política de seguridad.

### **2.2.8.2.3 RECOLECCIÓN DE EVIDENCIAS**

#### **Control**

Cuando una acción de seguimiento contra una persona u organización después de un incidente de la seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.

#### **Guía de implementación**

Se deberían desarrollar y cumplir procedimientos internos cuando se recolecta y se presenta evidencia con propósitos de acción disciplinaria dentro de la organización.

En general, las reglas para la evidencia comprenden los siguientes aspectos:

- a) Admisibilidad de la evidencia: si la evidencia se puede utilizar o no en la corte.
- b) Peso de la evidencia: la calidad y cabalidad de la evidencia.

Para lograr la admisibilidad de la evidencia, la organización debería asegurar que sus sistemas de información cumplen cualquier norma o código de práctica publicado para la producción de evidencia admisible.

El peso de la evidencia suministrada debería cumplir todos los requisitos aplicables.

Para lograr el peso de la evidencia, se debería demostrar la calidad y cabalidad de los controles empleados para proteger correcta y consistentemente la evidencia (es decir, evidencia del control del proceso) en todo el periodo en el cual la evidencia por recuperar se almacenó y procesó, mediante un rastreo sólido de la evidencia. En general, dicho rastreo sólido se puede establecer en las siguientes condiciones:

- a) Para documentos en papel: el original se guarda con seguridad con un registro de la persona que encontró el documento, el sitio en donde se encontró, la fecha en la cual se encontró y el testigo de tal hallazgo. toda investigación debería garantizar que los originales no han sido alterados.

- b) Para información en medios de computador: se deberían tomar duplicados o copias (dependiendo de los requisitos que se apliquen) de todos los medios removibles, la información en los discos duros o la memoria para garantizar la disponibilidad. es conveniente conservar el registro de todas las acciones durante el proceso de copiado y dicho proceso debería tener testigos. el medio y el registro originales (si no es posible, al menos un duplicado o copia) se deberían conservar intactos y de forma segura.

Todo el trabajo de peritaje se debería llevar a cabo únicamente en copias del material de evidencia. Se debería proteger la integridad de todo el material de evidencia.

El proceso de copia del material de evidencia debería estar supervisado por personal de confianza y se debería registrar la información sobre cuándo y cómo se realizó dicho proceso, quién ejecutó las actividades de copiado y qué herramientas o programas se utilizaron.

### **Información adicional**

Cuando un evento de la seguridad de la información se detecta inicialmente, es posible que no sea obvio si el evento llevará a una acción judicial. Por lo tanto, existe el peligro de destruir intencional o accidentalmente la evidencia necesaria antes de percatarse de la gravedad del incidente.

Es aconsejable la participación inicial de un abogado o de la policía en cualquier acción legal contemplada y asesorarse sobre la evidencia requerida.

La evidencia puede trascender las fronteras de la organización y/o las jurisdiccionales. En tales casos, se debería garantizar que la organización tiene derecho a recolectar la información requerida como evidencia.

Se deberían tener en cuenta los requisitos de las diferentes jurisdicciones para maximizar las oportunidades de admisión en las jurisdicciones correspondientes.



## **2.2.9 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**

### **2.2.9.1 ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**

Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.

Se debería implementar un proceso de gestión de la continuidad del negocio para minimizar el impacto y la recuperación por la pérdida de activos de información en la organización (la cual puede ser el resultado de, por ejemplo, desastres naturales, accidentes, fallas del equipo y acciones deliberadas) hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación.

En este proceso es conveniente identificar los procesos críticos para el negocio e integrar los requisitos de la gestión de la seguridad de la información de la continuidad del negocio con otros requisitos de continuidad relacionados con aspectos tales como operaciones, personal, materiales, transporte e instalaciones.

Las consecuencias de desastres, fallas de la seguridad, pérdida del servicio y disponibilidad del servicio se deberían someter a un análisis del impacto en el negocio. Se deberían desarrollar e implementar planes de continuidad del negocio para garantizar la restauración oportuna de las operaciones esenciales.

La seguridad de la información debería ser una parte integral de todo el proceso de continuidad del negocio y de otros procesos de gestión en la organización.

La gestión de la continuidad del negocio debería incluir controles para identificar y reducir los riesgos, además del proceso general de evaluación de riesgos, limitar las consecuencias de los incidentes dañinos y garantizar la disponibilidad de la información requerida para los procesos del negocio.

### **2.2.9.1.1 INCLUSIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN EL PROCESO DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**

#### **Control**

Se debería desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de la seguridad de la información necesarios para la continuidad del negocio de la organización.

#### **Guía de implementación**

El proceso debería reunir los siguientes elementos clave para la gestión de la continuidad del negocio:

- a) Comprensión de los riesgos que enfrenta la organización en términos de la probabilidad y el impacto en el tiempo, incluyendo la identificación y la determinación de la prioridad de los procesos críticos del negocio.
- b) Identificación de todos los activos involucrados en los procesos críticos del negocio.
- c) Comprensión del impacto que puedan tener las interrupciones causadas por incidentes de la seguridad de la información (es importante encontrar soluciones para manejar los incidentes que producen impactos menores, así como los incidentes graves que puedan amenazar la viabilidad de la organización), y establecer los objetivos del negocio para los servicios de procesamiento de información.
- d) Consideración de la adquisición de pólizas de seguros adecuadas que puedan formar parte de todo el proceso de continuidad del negocio y de la gestión de riesgos operativos.
- e) Identificación y consideración de la implementación de controles preventivos y mitigantes adicionales.

- f) Identificación de recursos financieros, organizacionales, técnicos y ambientales suficientes para tratar los requisitos identificados de la seguridad de la información.
- g) Garantizar la seguridad del personal y la protección de los servicios de procesamiento de información y de la propiedad de la organización.
- h) Formulación y documentación de los planes de continuidad del negocio que abordan los requisitos de la seguridad de la información acorde con la estrategia acordada de continuidad del negocio.
- i) Prueba y actualización regular de los planes y procesos establecidos.
- j) Garantizar que la gestión de la continuidad del negocio está incorporada en los procesos y la estructura de la organización. la responsabilidad por el proceso de gestión de la continuidad del negocio se debería asignar en un nivel apropiado en la organización.

#### **2.2.9.1.2 CONTINUIDAD DEL NEGOCIO Y EVALUACIÓN DE RIESGOS**

##### **Control**

Se deberían identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información.

##### **Guía de implementación**

Los aspectos de la seguridad de la información en la continuidad del negocio se deberían basar en la identificación de los eventos (o secuencia de eventos) que pueden causar interrupciones en los procesos del negocio de la organización, por ejemplo fallas de los equipos, errores humanos, robo, desastres naturales y actos terroristas. Se debería continuar con una evaluación de riesgos para determinar la probabilidad y el impacto de tales interrupciones, en términos de tiempo, escala de daño y periodo de recuperación.

Las evaluaciones de riesgos para la continuidad del negocio se deberían efectuar con la plena participación de los responsables de los recursos y los procesos del negocio. Estas evaluaciones deberían considerar todos los procesos del negocio sin limitarse a los servicios de procesamiento de información, sino incluir los resultados específicos para la seguridad de la información. Es importante vincular en conjunto todos los aspectos del riesgo para obtener un panorama completo de los requisitos de continuidad del negocio de la organización. Una evaluación debería identificar, cuantificar y priorizar los riesgos frente a los criterios y los objetivos pertinentes para la organización, incluyendo los recursos críticos, impactos de las interrupciones, duración permitida de corte y prioridades de recuperación.

Dependiendo de los resultados de una evaluación de riesgos, se debería desarrollar una estrategia de continuidad del negocio para determinar el enfoque global para la continuidad del negocio. Una vez que se ha creado esta estrategia, la dirección debería aprobarla y se debería crear y respaldar un plan para la implementación de esta estrategia.

#### **2.2.9.1.3 DESARROLLO E IMPLEMENTACIÓN DE PLANES DE CONTINUIDAD QUE INCLUYAN LA SEGURIDAD DE LA INFORMACIÓN**

##### **Control**

Se deberían desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requerido, después de la interrupción o la falla de los procesos críticos para el negocio.

##### **Guía de implementación**

En el proceso de planificación de la continuidad del negocio se deberían considerar los siguientes aspectos:

- a) Identificar y acordar todas las responsabilidades y los procedimientos para la continuidad del negocio.
- b) Identificar la pérdida aceptable de información y servicios.

- c) Implementar los procedimientos que permitan recuperar y restaurar las operaciones del negocio y la disponibilidad de la información en las escalas de tiempo requeridas. es necesario atender una evaluación de las dependencias internas y extremas del negocio y de los contratos establecidos.
- d) Procedimientos operativos que se han de seguir en espera de la terminación de la recuperación y restauración.
- e) Documentación de procedimientos y procesos acordados.
- f) Formación apropiada del personal en los procedimientos y procesos acordados, incluyendo el manejo de las crisis.
- g) Pruebas y actualización de los planes.

El proceso de planificación se debería centrar en los objetivos requeridos del negocio, por ejemplo la restauración de servicios de comunicación específicos para los clientes en un lapso de tiempo aceptable. Los servicios y recursos que lo facilitan deberían identificarse, incluyendo el personal, los recursos no relacionados con el procesamiento de información, al igual que las disposiciones de respaldo para los servicios de procesamiento de información. Estas disposiciones de respaldo pueden incluir arreglos con terceras partes en forma de acuerdos recíprocos o servicios de suscripción comercial.

Los planes de continuidad del negocio deberían afrontar las vulnerabilidades de la organización y, por lo tanto, pueden contener información sensible que es necesario proteger adecuadamente. Las copias de los planes de la continuidad del negocio se deberían almacenar en un lugar lejano, a suficiente distancia para escapar a cualquier daño por algún desastre en la sede principal. La dirección debería garantizar que las copias de los planes de continuidad del negocio están actualizadas y protegidas con el mismo nivel de la seguridad que se aplica en la sede principal. De igual modo, el otro material necesario para ejecutar los planes de continuidad se debería almacenar en un sitio lejano.

Si se utilizan lugares alternos temporales, el nivel de los controles de la seguridad implementados en estos lugares debería ser equivalente al de la sede principal.

## **Información adicional**

Es conveniente observar que los planes y las actividades de la gestión de crisis pueden ser diferentes de la gestión de la continuidad del negocio, es decir, se puede presentar una crisis que se pueda adaptar con procedimientos de gestión normales.

### **2.2.9.1.4 ESTRUCTURA PARA LA PLANIFICACIÓN DE LA CONTINUIDAD DEL NEGOCIO**

#### **Control**

Se debería mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento.

#### **Guía de implementación**

Cada plan de continuidad del negocio debería describir el enfoque para la continuidad, por ejemplo el enfoque para garantizar la disponibilidad y seguridad de la información o del sistema de información. Igualmente, cada plan debería especificar el plan de escalada y las condiciones para su activación, así como las personas responsables de ejecutar cada componente del plan.

Cuando se identifican nuevos requisitos, todos los procedimientos de emergencia existentes, por ejemplo planes de evacuación o disposiciones de respaldo, se deberían modificar apropiadamente.

Los procedimientos se deberían incluir en el programa de gestión de cambios de la organización para garantizar el tratamiento adecuado de los aspectos de la continuidad el negocio.

Cada plan debería tener un responsable específico. Los procedimientos de emergencia, los planes de recursos de emergencia manuales y de reanudación deberían ser responsabilidad de los responsables de los recursos o procesos apropiados del negocio involucrados. Las disposiciones de respaldo para los servicios técnicos alternos, como servicios de procesamiento de información y comunicaciones, usualmente deberían ser responsabilidad de los proveedores del servicio.

Una estructura para la planificación de la continuidad del negocio debería abordar los requisitos de la seguridad de la información identificados y considera los siguientes aspectos:

- a) Las condiciones para la activación de los planes que describen el proceso a seguir (por ejemplo, la forma de evaluar la situación y quién se va a involucrar) antes de activar cada plan.
- b) Los procedimientos de emergencia que describen las acciones por realizar tras un incidente que ponga en peligro las operaciones del negocio.
- c) Los procedimientos de respaldo que describen las acciones por realizar para desplazar las actividades esenciales del negocio o los servicios de soporte a lugares temporales alternos y para devolver la operatividad de los procesos del negocio en los plazos requeridos.
- d) Los procedimientos operativos temporales por seguir mientras se terminan la recuperación y la restauración.
- e) Los procedimientos de reanudación que describen las acciones por realizar para que las operaciones del negocio vuelvan a la normalidad.
- f) Una programación de mantenimiento que especifique cómo y cuándo se realizarán pruebas al plan y el proceso para el mantenimiento del plan.
- g) Actividades de concienciación, educación y formación diseñadas para comprender los procesos de continuidad del negocio y garantizar que los procesos siguen siendo eficaces.

- h) Las responsabilidades de las personas, que describan quién es responsable de la ejecución de cada componente del plan. Si se requiere, se deberían nombrar suplentes.
- i) Los activos y recursos críticos necesarios para ejecutar los procedimientos de emergencia, respaldo y reanudación.

#### **2.2.9.1.5 PRUEBAS, MANTENIMIENTO Y REEVALUACIÓN DE LOS PLANES DE CONTINUIDAD DEL NEGOCIO**

##### **Control**

Los planes de continuidad del negocio se deberían someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia.

##### **Guía de implementación**

Las pruebas del plan de continuidad del negocio deberían asegurar que todos los miembros del equipo de recuperación y otro personal pertinente son conscientes de los planes y sus responsabilidades para la continuidad del negocio y la seguridad de la información, y conocen su función cuando se ejecuta un plan.

La programación de las pruebas para los planes de continuidad del negocio debería indicar cómo y cuándo se va a probar cada elemento del plan. Cada uno de los elementos se debería probar con frecuencia.

Es conveniente utilizar una variedad de técnicas para garantizar que los planes funcionarán en condiciones reales. Éstas incluirían:

- a) La prueba sobre papel de varios escenarios (analizando las disposiciones de recuperación con ayuda de ejemplos de interrupciones).
- b) Las simulaciones (particularmente para la formación del personal en sus funciones de gestión de crisis / post-incidentes).



- c) Las pruebas de recuperación técnica (garantizando que los sistemas de información se pueden restaurar eficazmente).
- d) Las pruebas de recuperación en un lugar alternativo (ejecutando procesos del negocio en paralelo con las operaciones de recuperación fuera de la sede principal).
- e) Las pruebas de los recursos y servicios del proveedor (asegurando que los servicios y productos proporcionados externamente cumplirán el compromiso contraído).
- f) Los ensayos completos (probando que la organización, el personal, el equipo, las instalaciones y los procesos pueden hacer frente a las interrupciones).

Cualquier organización puede utilizar estas técnicas. Éstas se deberían aplicar de forma pertinente para el plan específico de recuperación. Se deberían registrar los resultados de las pruebas y, cuando sea necesario, tomar las acciones para mejorar los planes.

Se debería asignar responsabilidad para las revisiones regulares de cada plan de continuidad del negocio. La identificación de los cambios en las disposiciones del negocio que aún no se reflejan en los planes de continuidad del negocio debería ir seguida de una actualización adecuada del plan. Este proceso formal de control de cambios debería garantizar la distribución y el refuerzo de los planes actualizados mediante revisiones regulares del plan completo.

Los ejemplos de los cambios en donde se debería considerar la actualización de los planes de continuidad el negocio incluyen la adquisición de equipos nuevos, la mejora de los sistemas y cambios en:

- a) El personal.
- b) Las direcciones o los números telefónicos.
- c) La estrategia del negocio.
- d) Los lugares, dispositivos y recursos.

- e) La legislación.
- f) Los contratistas, proveedores y clientes principales.
- g) Los procesos existentes, nuevos o retirados.
- h) Los riesgos (operativos y financieros).

## **2.2.10 CUMPLIMIENTO**

### **2.2.10.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES**

Evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de la seguridad.

El diseño, el uso, la operación y la gestión de los sistemas de información pueden estar sujetos a requisitos de la seguridad estatutarios, reglamentarios y contractuales.

Se debería buscar asesoría sobre los requisitos legales específicos de los asesores jurídicos de la organización o de abogados practicantes calificados. Los requisitos legales varían de un país a otro y pueden variar para la información creada en un país y que se transmite a otro (es decir, el flujo de datos transfronterizo).

#### **2.2.10.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE**

##### **Control**

Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deberían definir explícitamente, documentar y mantener actualizados para cada sistema de información y para la organización.

## **Guía de implementación**

Los controles específicos y las responsabilidades individuales para cumplir estos requisitos se deberían definir y documentar de forma similar

### **2.2.10.1.2 DERECHOS DE PROPIEDAD INTELECTUAL (DPI)**

#### **Control**

Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.

#### **Guía de implementación**

Se deberían tomar en consideración las siguientes directrices para proteger todo material que se pueda considerar propiedad intelectual:

- a) Publicar una política de cumplimiento de los derechos de propiedad intelectual que defina el uso legal del software y de los productos de información.
- b) Adquirir software únicamente a través de fuentes conocidas y de confianza para garantizar que no se violan los derechos de copia.
- c) Mantener la concienciación sobre las políticas para proteger los derechos de propiedad intelectual y notificar la intención de tomar acciones disciplinarias para el personal que los viole.
- d) Mantener registros apropiados de los activos e identificar todos los activos con requisitos para proteger los derechos de propiedad intelectual.
- e) Mantener prueba y evidencia sobre la propiedad de licencias, discos maestros, manuales, etc.

- f) Implementar controles para asegurar que no se excede el número máximo de usuarios permitidos.
- g) Verificar que únicamente se instalan software autorizado y productos con licencia.
- h) Suministrar una política para mantener las condiciones de licencia apropiadas.
- i) Suministrar una política para la disposición o transferencia de software a otros.
- j) Usar las herramientas de auditoría adecuadas.
- k) Cumplir los términos y condiciones para el software y la información obtenidos de redes públicas.
- l) No duplicar, convertir en otro formato ni extraer de grabaciones comerciales (película, audio) diferentes a los permitidos por la ley de derechos de copia.
- m) No copiar total ni parcialmente libros, artículos, informes ni otros documentos diferentes a los permitidos por la ley de derechos de copia.

### **Información adicional**

Los derechos de propiedad intelectual incluyen derechos de copia de software o de documentos, derechos de diseño, marcas registradas, patentes y licencias de códigos fuente.

Los productos de software patentados usualmente se suministran bajo un acuerdo de licencia que especifica los términos y condiciones de la licencia, por ejemplo, limitar el uso de los productos a máquinas específicas o limitar el copiado a la creación de copias de respaldo únicamente. La situación de DPI del software desarrollado por la organización requiere ser aclarada con el personal.

Los requisitos legales, reglamentarios y contractuales pueden imponer restricciones a la copia de material patentado. En particular pueden exigir que únicamente se utilice el material desarrollado por la organización o que tenga licencia y es suministrado a la organización por quien lo desarrolla. La violación de los derechos de copia puede conducir a acciones legales que pueden implicar procedimientos judiciales.

### **2.2.10.1.3 PROTECCIÓN DE LOS REGISTROS DE LA ORGANIZACIÓN**

#### **Control**

Los registros importantes se deberían proteger contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y del negocio.

#### **Guía de implementación**

Los registros se deberían clasificar en tipos de registro, por ejemplo registros de contabilidad, registros de bases de datos, registros de transacciones, registros de auditoría y procedimientos operativos, cada uno con detalles de los periodos de retención y los tipos de medio de almacenamiento como papel, microfichas, medios magnéticos, ópticos, etc. Todo material relacionado con claves criptográficas y programas asociados con archivos encriptados o firmas digitales, también se debería almacenar para permitir el descifrado de los registros durante el periodo de tiempo durante el cual se retienen los registros.

Es conveniente tomar en consideración la posibilidad de deterioro de los medios utilizados para almacenar los registros. Los procedimientos de almacenamiento y manipulación se deberían implementar según las recomendaciones del fabricante. Para almacenamiento a largo plazo, se recomienda considerar el uso de papel y microfichas.

Al seleccionar los medios de almacenamiento electrónico, se deberían incluir los procedimientos para garantizar la capacidad de acceso a los datos (facilidad tanto del medio como del formato) durante todo el periodo de retención para salvaguardar contra pérdida debido a cambio en la tecnología futura.

Los sistemas de almacenamiento de datos se deberían seleccionar de forma tal que los datos requeridos se puedan recuperar en el periodo de tiempo y el formato aceptable, dependiendo de los requisitos que se deben cumplir.

El sistema de almacenamiento y manipulación debería garantizar la identificación de los registros y de su periodo de retención tal como se define en los reglamentos o la legislación nacional o regional, si se aplica. Este sistema debería permitir la destrucción adecuada de los registros después de este periodo, si la organización no los necesita.

Para cumplir estos objetivos de salvaguarda de registros, la organización debería seguir los siguientes aspectos:

- a) Se deberían publicar directrices sobre retención, almacenamiento, manipulación y eliminación de registros e información.
- b) Es conveniente publicar una programación de retención que identifique los registros y el periodo de tiempo de su retención.
- c) Se recomienda conservar un inventario de las fuentes de información clave.
- d) Se deberían implementar los controles apropiados para proteger los registros y la información contra pérdida, destrucción y falsificación.

### **Información adicional**

Puede ser necesario retener algunos registros de manera segura para cumplir requisitos estatutarios, reglamentarios o contractuales, así como para dar soporte a las actividades esenciales del negocio. Los ejemplos incluyen los registros que se pueden necesitar como evidencia de que la organización funciona cumpliendo las reglas estatutarias o reglamentarias, para garantizar la defensa adecuada contra potenciales acciones civiles o criminales o para confirmar el estado financiero de la organización con respecto a socios, terceras partes y auditores. El periodo de tiempo y el contenido de los datos para la retención de información pueden ser establecidos por la ley o la reglamentación nacional.

#### **2.2.10.1.4 PROTECCIÓN DE LOS DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL**

##### **Control**

Se debería garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato.

## **Guía de implementación**

Se debería desarrollar e implementar una política de protección y privacidad de los datos. Esta política se debería comunicar a todas las personas involucradas en el procesamiento de información personal.

El cumplimiento de esta política y de todos los reglamentos y leyes pertinentes a la protección de datos requiere estructura y control adecuados de gestión. Con frecuencia esto se logra mejor nombrando a una persona responsable, como por ejemplo un funcionario para protección de datos, quien debería brindar guía a directores, usuarios y proveedores de servicios sobre sus responsabilidades individuales y los procedimientos específicos que se deberían seguir. La responsabilidad del manejo de la información personal y de la concienciación sobre los principios de protección de datos debería estar acorde con los reglamentos y la legislación correspondientes. Se deberían implementar medidas técnicas y organizacionales apropiadas.

### **Información adicional**

Varios países han introducido leyes que imponen controles a la recolección, el procesamiento y la transmisión de datos personales (generalmente se trata de información sobre personas vivas que pueden ser identificadas a partir de tal información).

Dependiendo de la respectiva legislación nacional, estos controles pueden imponer funciones sobre aquellos que recolectan, procesan y distribuyen información personal y pueden restringir la capacidad de transferencia de datos a otros países.

#### **2.2.10.1.5 PREVENCIÓN DEL USO INADECUADO DE LOS SERVICIOS DE PROCESAMIENTO DE INFORMACIÓN**

##### **Control**

Se debería disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados.

## **Guía de implementación**

La dirección debería aprobar el uso de los servicios de procesamiento de información.

Todo uso de estos servicios para propósitos no relacionados con el negocio sin autorización de la dirección, o para cualquier propósito no autorizado se debería considerar uso inadecuado de los servicios. Si se identifica alguna actividad no autorizada por medio de monitoreo u otros medios, esta actividad debería llamar la atención del director correspondiente para estudiar la acción legal y/o disciplinaria adecuada.

Antes de implementar los procedimientos de monitoreo se debería tener asesoría legal.

Todos los usuarios deberían conocer el alcance preciso de su acceso permitido y del monitoreo implementado para detectar el uso no autorizado. Esto se puede lograr dando a los usuarios autorización escrita, una copia de la cual debería estar firmada por el usuario y la organización debería conservarla. A los empleados de la organización, contratistas y usuarios de terceras partes se les debería advertir que no se permitirá acceso que no esté autorizado.

En el momento del registro de inicio, se debería presentar un mensaje de advertencia que indique que el servicio de procesamiento de información al cual se está ingresando es propiedad de la organización y que no se permite el acceso no autorizado. El usuario debe reconocer y reaccionar apropiadamente al mensaje de la pantalla para continuar con el proceso de registro de inicio.

### **Información adicional**

Los servicios de procesamiento de información de la organización tienen el fin principal o exclusivo de los propósitos del negocio.

La detección de intrusión, la inspección del contenido y otras herramientas de monitoreo pueden ayudar y evitar el uso inadecuado de los servicios de procesamiento de información.

Muchos países tienen legislaciones que protegen contra el uso inadecuado del computador.



Puede ser un acto criminal usar el computador con propósitos no autorizados.

La legalidad de monitorear la utilización varía de un país a otro y puede exigir que la dirección advierta a los usuarios sobre tal monitoreo y/o obtenga su acuerdo. Cuando el sistema al cual se ingresa se utiliza para acceso público (por ejemplo en un servidor web público) y está sujeto a monitoreo de la seguridad, se debería mostrar un mensaje que así lo indique.

#### **2.2.10.1.6 REGLAMENTACIÓN DE LOS CONTROLES CRIPTOGRÁFICOS**

##### **Control**

Se deberían utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.

##### **Guía de implementación**

Se recomienda tener presentes los siguientes elementos para el cumplimiento con acuerdos, leyes y reglamentos pertinentes:

- a) Restricción de importaciones y/o exportaciones de hardware y software de computadores para la ejecución de funciones criptográficas.
- b) Restricción de importaciones y/o exportaciones de hardware y software de computadores diseñados para adicionarles funciones criptográficas.
- c) Restricciones al uso de encriptación.
- d) Métodos obligatorios o discrecionales de acceso por parte de las autoridades del país a la información encriptada mediante hardware o software para brindar confidencialidad al contenido.

Se debería buscar asesoría legal para garantizar el cumplimiento con las leyes y los reglamentos nacionales. Antes de desplazar la información encriptada o los controles criptográficos a otros países, se debería tener asesoría legal.

## **2.2.10.2 CUMPLIMIENTO DE LAS POLÍTICAS Y LAS NORMAS DE LA SEGURIDAD Y CUMPLIMIENTO TÉCNICO**

Asegurar que los sistemas cumplen con las normas y políticas de la seguridad de la organización.

La seguridad de los sistemas de información se debería revisar a intervalos regulares.

Dichas revisiones se deberían llevar a cabo frente a las políticas de la seguridad apropiadas y se deberían auditar las plataformas técnicas y los sistemas de información para determinar el cumplimiento de las normas aplicables sobre implementación de la seguridad y los controles de la seguridad documentados.

### **2.2.10.2.1 CUMPLIMIENTO CON LAS POLÍTICAS Y LAS NORMAS DE LA SEGURIDAD**

#### **Control**

Los directores deberían garantizar que todos los procedimientos de la seguridad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento con las políticas y las normas de la seguridad.

#### **Guía de implementación**

Los directores deberían revisar con regularidad en su área de responsabilidad el cumplimiento del procesamiento de información con las políticas de la seguridad adecuadas, las normas y cualquier otro requisito de la seguridad.

Si se halla algún incumplimiento como resultado de la revisión, los directores deberían:

- a) Determinar la causa del incumplimiento.
- b) Evaluar la necesidad de acciones para garantizar que no se presenten incumplimientos.
- c) Determinar e implementar la acción correctiva apropiada,

d) Revisar la acción correctiva que se ejecutó.

Se deberían registrar los resultados de las revisiones y las acciones correctivas llevadas a cabo por los directores y conservar dichos registros. Los directores deberían informar de los resultados a las personas que realizan revisiones independientes, cuando la revisión independiente tiene lugar en el área de su responsabilidad.

## **2.2.10.2.2 VERIFICACIÓN DEL CUMPLIMIENTO TÉCNICO**

### **Control**

Los sistemas de información se deberían verificar periódicamente para determinar el cumplimiento con las normas de implementación de la seguridad.

### **Guía de implementación**

La verificación del cumplimiento técnico se debería realizar bien sea manualmente (con soporte de las herramientas de software apropiadas, si es necesario) por un ingeniero de sistemas con experiencia y/o con la ayuda de herramientas automáticas que generan un informe técnico para la interpretación posterior por parte del especialista técnico.

Si se utilizan evaluaciones de vulnerabilidad o pruebas de penetración, se recomienda tener cuidado puesto que dichas actividades pueden poner en peligro la seguridad del sistema. Tales pruebas se deberían planificar, documentar y ser repetibles.

La verificación del cumplimiento técnico únicamente la deberían realizar personas autorizadas y competentes o bajo supervisión de dichas personas.

### **Información adicional**

La verificación del cumplimiento técnico involucra el examen de los sistemas operativos para asegurar que los controles de hardware y software se han implementado correctamente. Este tipo de verificación del cumplimiento requiere experiencia técnica especializada.

La verificación del cumplimiento también comprende, por ejemplo pruebas de penetración y evaluaciones de la vulnerabilidad, las cuales pueden ser realizadas por expertos independientes especialmente contratados para este propósito. Ello puede ser útil para detectar vulnerabilidades en el sistema y verificar qué tan efectivos son los controles evitando el acceso no autorizado debido a estas vulnerabilidades.

Las pruebas de penetración y las evaluaciones de vulnerabilidad proveen una visión instantánea de un sistema en un estado específico en un momento específico. Esta instantánea se limita a aquellas porciones del sistema que se someten a prueba real durante el (los) intento (s) de penetración. Las pruebas de penetración y las evaluaciones de vulnerabilidad no substituyen a una evaluación de riesgos.

### **2.2.10.3 CONSIDERACIONES DE LA AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN**

Maximizar la eficacia de los procesos de auditoría de los sistemas de información y minimizar su interferencia.

Deberían existir controles para salvaguardar los sistemas operativos y las herramientas de auditoría durante las auditorías de los sistemas de información.

También se requiere protección para salvaguardar la integridad y evitar el uso inadecuado de las herramientas de auditoría.

#### **2.2.10.3.1 CONTROLES DE AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN**

##### **Control**

Los requisitos y las actividades de auditoría que implican verificaciones de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos del negocio.

##### **Guía de implementación**

Se deberían tener presente las siguientes directrices:

- a) Los requisitos de auditoría se deberían acordar con la dirección correspondiente.
- b) Se debería acordar y controlar el alcance de las verificaciones.
- c) Las verificaciones se deberían limitar al acceso de sólo lectura del software y los datos.
- d) el acceso diferente al de sólo lectura únicamente se debería permitir para copias aisladas de archivos del sistema que se puedan borrar al terminar la auditoría, o se debería dar protección adecuada, si existe la obligación de conservar dichos archivos según los requisitos de documentación de la auditoría.
- e) Los recursos para llevar a cabo las verificaciones se deberían identificar explícitamente y estar disponibles.
- f) Se deberían identificar y acordar los requisitos para el procesamiento especial o adicional.
- g) Todo acceso se debería monitorear y registrar para crear un rastro para referencia. el uso de rastros de referencia de tiempo se debería considerar para datos o sistemas críticos.
- h) Se recomienda documentar todos los procedimientos, requisitos y responsabilidades.
- i) La persona que realiza la auditoría debería ser independiente de las actividades auditadas.

#### **2.2.10.3.2 PROTECCIÓN DE LAS HERRAMIENTAS DE AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN**

##### **Control**

Se debería proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar su uso inadecuado o ponerlas en peligro.

## **Guía de implementación**

Las herramientas de auditoría de los sistemas de información, por ejemplo, software o archivos de datos, se deberían separar de los sistemas operativos y de desarrollo y no mantenerse en librerías de cinta, salvo que se les proporcione un nivel adecuado de protección adicional.

## **CAPÍTULO III**

### **3 MANUAL DE POLÍTICAS DE SEGURIDAD**

Este manual de políticas de seguridad es elaborado de acuerdo al análisis de riesgos y vulnerabilidades en las direcciones de la Empresa Eléctrica Regional Norte S.A. – EMELNORTE, por consiguiente el alcance de estas políticas, se encuentra sujeto a la empresa.

#### **3.1 ACTIVOS**

Toda adquisición de tecnología informática se efectuará a través del Departamento de Adquisiciones (Portal de Compras Públicas) previo a un requerimiento de usuario y la respectiva autorización del Director correspondiente, deberá constar en el presupuesto.

La adquisición de bienes informáticos, quedará sujeta a los lineamientos establecidos en esta política.

##### **3.1.1 DE INFORMACIÓN**

La Dirección de Tecnologías de la Información y Comunicación tiene como objetivo asegurar que la información recibe el nivel de protección adecuado. La información se debería clasificar para indicar la necesidad, las prioridades y el grado esperado de protección al manejar la información.

La información tiene diferentes grados de sensibilidad e importancia. Algunos elementos pueden requerir un grado adicional de protección o manejo especial. Se recomienda utilizar un esquema de clasificación de la información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas especiales de manejo.

La información que cada usuario mantiene en sus equipos es de su responsabilidad, la Dirección de Tecnologías de la Información y Comunicación, no se responsabilizará en caso de pérdida de la misma.

### **3.1.2 DE SOFTWARE, FÍSICOS Y SERVICIOS**

La Dirección de Tecnologías de la Información y Comunicación, al planear las operaciones relativas a la adquisición de bienes informáticos y/o servicios, establecerá prioridades y en su selección deberá tomar en cuenta: estudio técnico, precio, calidad, experiencia, desarrollo tecnológico, estándares y capacidad, entendiéndose por:

#### **Precio**

Costo inicial, costo de mantenimiento y consumibles por el período estimado de uso de los equipos;

#### **Calidad**

Parámetro cualitativo que especifica las características técnicas de los recursos informáticos.

#### **Experiencia**

Presencia en el mercado nacional e internacional, estructura de servicio, la confiabilidad de los bienes y certificados de calidad con los que se cuente.

#### **Desarrollo Tecnológico**

Se deberá analizar su vida útil, su nivel tecnológico con respecto a la oferta existente y su permanencia en el mercado.

#### **Capacidades**

Se deberá analizar si satisface la demanda actual con un margen de holgura y capacidad de crecimiento para soportar la carga de trabajo del área.

Los Recursos Informáticos, Datos, Software, Red Corporativa y Sistemas de Comunicación Electrónica están disponibles exclusivamente para cumplir las obligaciones y propósito de la operación para la que fueron diseñados e implantados.

Todos los usuarios de dichos recursos deben saber que no tiene el derecho de confidencialidad en su uso.



El introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, inmorales u ofensivos, será motivo de sanción para los funcionarios, de acuerdo a la normativa vigente.

Perturbar el trabajo de los demás enviando mensajes o archivos que puedan inferir en el trabajo de otro usuario de la red, incurrirá en la aplicación de la sanción según la normativa vigente.

El diseminar “virus”, “gusanos”, “troyanos” y otros tipos de programas dañinos para los sistemas de procesos de la información, será motivo de sanción.

## **3.2 EQUIPOS DE CÓMPUTO**

### **3.2.1 DE LA INSTALACIÓN**

La instalación del equipo de cómputo, quedará sujeta a los siguientes lineamientos:

Los equipos para uso interno se instalarán en lugares adecuados, lejos de polvo y alto tráfico de personas.

Todo equipo de cómputo, que esté o sea conectado a la red de EMELNORTE, o aquel que en forma autónoma se tenga y que sea propiedad de la institución debe sujetarse a las normas y procedimientos de instalación que emite La Dirección de Tecnologías de la Información y Comunicación.

La Dirección de TIC's deberá contar con un plano actualizado de las instalaciones eléctricas y de comunicaciones.

Las instalaciones eléctricas y de comunicaciones, estarán de preferencias fijas o en su defecto resguardadas del paso de personas o máquinas, y libres de cualquier interferencia eléctrica o magnética.

Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.

En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.

Los equipos informáticos mantendrán una estandarización en los nombres que se le asigne, cumpliendo con las necesidades de la Dirección de TIC's. El nombre no debe exceder de 15 caracteres.

El formato de nombres de los equipos de cómputo (computadores de escritorio, portátiles) sería el siguiente:

10IBATICSOP-16

10: ÁREA REFERENCIAL CÓDIGO PROVINCIAL

IBA: CIUDAD, CANTÓN DE UBICACIÓN DE LA EMPRESA O SUCURSAL

TIC: CORRESPONDE A LA DIRECCIÓN

SOP: ÁREA DE LA DIRECCIÓN

16: CUARTO OCTETO DE LA DIRECCIÓN IP

Para el caso de impresoras será el siguiente formato indicado:

10IBATICIMP-24

10: ÁREA REFERENCIAL CÓDIGO PROVINCIAL

IBA: CIUDAD, CANTÓN DE UBICACIÓN DE LA EMPRESA O SUCURSAL

TIC: CORRESPONDE A LA DIRECCIÓN, AREA O DEPARTAMENTO

IMP: INDICA QUE ES UNA IMPRESORA

24: CUARTO OCTETO DE LA DIRECCIÓN IP

Para el caso de cámaras de video vigilancia será el siguiente:

IBMATPB20-51

IBA: CIUDAD, CANTÓN DE UBICACIÓN DE LA EMPRESA O SUCURSAL

MAT: NOMBRE DE LA SUCURSAL

PB: UBICACIÓN FISICA

20: CUARTO OCTETO DE LA DIRECCIÓN IP

51: VLAN ASIGNADA

Los formatos para los nombres de los equipos informáticos debe actualizarse periódicamente por la Dirección de TIC's.

### **3.2.2 PARA EL MANTENIMIENTO**

Es obligación de la Dirección de TIC's vigilar que el equipo de cómputo se use bajo las condiciones especificadas por el proveedor y de acuerdo a las funciones del área a la que se asigne.

Los empleados de la empresa al usar el equipo de cómputo, se abstendrán de consumir alimentos, fumar o realizar actos que perjudiquen el funcionamiento del mismo o deterioren la información almacenada en medios magnéticos, ópticos, o medios de almacenamiento removibles de última generación.

A la Dirección de TIC's corresponde la realización del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física y su acondicionamiento específico a que tenga lugar. Para tal fin debe emitir las normas y procedimientos respectivos.

Los responsables la Dirección de Tecnologías de la Información y Comunicación son los únicos autorizados para realizar mantenimiento preventivo y correctivo, o para autorizar el mantenimiento por parte de terceros.

### **3.2.3 DE LA ACTUALIZACIÓN**

La Dirección de TIC's es responsable de mantener versiones actualizadas de los sistemas usados en EMELNORTE, para ello se realizará un plan adecuado y a tiempo de las actualizaciones respectivas.

Todo equipo de cómputo (computadoras personales, estaciones de trabajo, supercomputadora y demás relacionados) y los de telecomunicaciones que sean propiedad de la empresa debe procurarse sean actualizados tendiendo a conservar e incrementar la calidad del servicio que presta, mediante la mejora sustantiva de su desempeño.

Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente a la Dirección de Tecnologías de la Información y Comunicación para que tomen las medidas correctivas al problema.

### **3.2.4 DE LA RE-UBICACIÓN**

La reubicación de los equipos de cómputo se realizará satisfaciendo las normas y procedimientos que para ello emita la Dirección de Tecnologías de la Información y Comunicación.

En caso de existir personal técnico de apoyo, este notificará de los cambios tanto físicos como de software que realice la Dirección de Tecnologías de la Información y Comunicación y al procedimiento de ALMACENAMIENTO, ASEGURAMIENTO E INVENTARIOS notificando también los cambios de los equipos para adjuntarlos al inventario.

El equipo de cómputo a reubicar se hará únicamente bajo la autorización del responsable, contando el lugar a donde se hará la ubicación con los medios necesarios para la instalación del equipo.

Es responsabilidad de cada usuario informar a la Dirección de TIC's, mediante hojas de requerimiento la necesidad de reubicar los equipos para dar la asistencia correspondiente.

### **3.2.5 DE LA SEGURIDAD**

Cada usuario es responsable de mantener sus claves de seguridad en secreto.

Los equipos de la Empresa sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.

Cualquier falla en los computadores o en la red debe reportarse inmediatamente a la Dirección de Tecnologías de la Información y Comunicación para lograr evitar problemas serios como pérdida de la información o indisponibilidad de los servicios.

No deben usarse dispositivos de almacenamiento en cualquier computadora de la Empresa sin que previamente se haya verificado que están libres de cualquier tipo de virus.

Los usuarios de PCs son responsables de realizar periódicamente el respaldo de los datos guardados en sus PCs, para evitar pérdidas de información.

Los usuarios de PCs son responsables de proteger los programas y datos contra pérdida o daño.

El personal que utiliza un computador portátil que contenga información confidencial de la Empresa, debe protegerlo y evitar el acceso a la información de personas no autorizadas.

Para prevenir el acceso no autorizado, utilice contraseñas difíciles de predecir y además debe configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además, cada vez que deba ausentarse de su oficina debe activar el protector de pantalla manualmente.

Para prevenir el ataque de virus, no está permitido el uso de módems de internet de cualquier operadora en los equipos de EMELNORTE que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la red interna de la Empresa.

Debe respetarse y no modificar la configuración de hardware y software establecida por la Dirección de Tecnologías de la Información y Comunicación.

Está terminantemente prohibido hacer copias o usar software de EMELNORTE para fines personales.

Los usuarios no deben copiar a un dispositivo de almacenamiento externo, el software de las computadoras de la Empresa, sin la aprobación previa de la Dirección de Tecnologías de la Información y Comunicación.

No debe utilizarse software descargado de Internet o software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por la Dirección de Tecnologías de la Información y Comunicación.

Se prohíbe estrictamente la instalación de software no autorizado, sin que haya sido previamente aprobado por la Dirección de Tecnologías de la Información y Comunicación, con el fin de prevenir la introducción de virus informáticos.

El internet es estrictamente para uso de las actividades propias de la Empresa y su uso será autorizado por la Presidencia Ejecutiva.

Queda totalmente prohibido, sacar los equipos de computación de la Empresa sin previa autorización por parte del director de cada dependencia. En caso de ser necesario sacar los mismos, se debe llenar el formulario de movilización de equipos y entregar al personal de seguridad.

### **3.3 COMUNICACIONES Y OPERACIONES**

#### **3.3.1 PROCEDIMIENTOS Y RESPONSABILIDADES**

El objetivo de la Dirección de Tecnologías de la Información y Comunicación es asegurar la operación correcta y segura de los servicios de procesamiento de información.

Se deberían establecer todas las responsabilidades y los procedimientos para la gestión y operación de todos los servicios de procesamiento de información. Esto incluye el desarrollo de procedimientos operativos apropiados.

Cuando sea conveniente, se debería implementar la separación de funciones para reducir el riesgo de uso inadecuado deliberado o negligente del sistema.

#### **3.3.2 PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA**

La Dirección de Tecnologías de la Información y Comunicación pretende minimizar el riesgo de fallas en los sistemas.

Se requieren una previa planificación y preparación para garantizar la disponibilidad de la capacidad y los recursos adecuados para entregar el desempeño requerido del sistema.

Es necesario hacer proyecciones de la capacidad futura para reducir el riesgo de sobrecarga del sistema.

Los requisitos operativos de los sistemas nuevos se deberían establecer, documentar y probar antes de su aceptación y uso.

### **3.3.3 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS Y MÓVILES**

La Dirección de Tecnologías de la Información y Comunicación busca proteger la integridad del software y de la información.

Se requieren precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no autorizados.

El software y los servicios de procesamiento de información son vulnerables a la introducción de códigos maliciosos tales como virus de computador, gusanos en la red, caballos troyanos y bombas lógicas. Los usuarios deberían ser conscientes de los peligros de los códigos maliciosos. Los directores deberían, cuando sea apropiado, coordinar con la dirección de TIC's los controles para evitar, detectar y retirar los códigos maliciosos y controlar los códigos móviles.

Se encuentra prohibida la conexión de equipos móviles, que no sean de la empresa, a la red interna de EMELNORTE, a menos de que exista la respectiva autorización de la Presidencia Ejecutiva.

### **3.3.4 RESPALDO**

La Dirección de Tecnologías de la Información y Comunicación pretende mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.

Se deberían establecer procedimientos de rutina para implementar la política y la estrategia de respaldo acordada para hacer copias de la seguridad de los datos y probar sus tiempos de restauración.

El personal responsable de mantener los servicios informáticos operativos, deberá sacar respaldos de la información de forma mensual y almacenarlos en un lugar seguro.

### **3.3.5 SEGURIDAD EN LAS REDES**

La Dirección de Tecnologías de la Información y Comunicación busca asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

La gestión segura de las redes, las cuales pueden sobrepasar las fronteras de la organización, exige la consideración cuidadosa del flujo de datos, las implicaciones legales, el monitoreo y la protección.

También pueden ser necesarios los controles adicionales para proteger la información sensible que pasa por las redes públicas.

### **3.3.6 MANEJO DE LOS MEDIOS**

La Dirección de Tecnologías de la Información y Comunicación trata de evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del negocio.

Estos medios se deberían controlar y proteger de forma física.

Se deberían establecer procedimientos operativos adecuados para proteger documentos, medios de computador (por ejemplo cintas, discos), datos de entrada/salida y documentación del sistema contra divulgación, modificación, remoción y destrucción no autorizadas.

### **3.3.7 MONITOREO**

La Dirección de Tecnologías de la Información y Comunicación pretende detectar actividades de procesamiento de la información no autorizadas.



Se deberían monitorear los sistemas y registrar los eventos de la seguridad de la información. Los registros de operador y la actividad de registro de fallas se deberían utilizar para garantizar la identificación de los problemas del sistema de información.

Una organización debería cumplir todos los requisitos legales pertinentes que se aplican a sus actividades de monitoreo y registro.

Debería emplearse el monitoreo del sistema para verificar la eficacia de los controles adoptados y revisar el cumplimiento de un modelo de política de acceso.

## **3.4 CONTROL DE ACCESO**

### **3.4.1 GESTIÓN DEL ACCESO DE LOS USUARIOS**

Todos los usuarios con acceso a un sistema de información o a una red informática, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.

Ningún usuario recibirá un identificador de acceso a la Red de Comunicaciones, Recursos Informáticos o Aplicaciones hasta que no acepte formalmente la Política de Seguridad vigente.

Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por el responsable de la información.

La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.

Los identificadores para usuarios temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.

Cada usuario, dispondrá de un identificador único, el cual se corresponde con la cuenta de usuario.

A cada identificador de usuario corresponderá una, y solo una persona física.

Todas aquellas operaciones realizadas por un usuario, serán siempre atribuidas al identificador utilizado que se hubiere identificado ante el sistema de información.

La Dirección de TIC's, realizará mensualmente, la actualización de usuarios, en coordinación con la Dirección de Talento Humano.

### **3.4.2 RESPONSABILIDAD DE LOS USUARIOS**

Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.

Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.

Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.

Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar a su jefe inmediato y éste reportar al responsable de la administración de la red.

El Usuario debe utilizar una contraseña compuesta por un mínimo de ocho caracteres constituida por una combinación de caracteres alfabéticos, numéricos y especiales.

La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos.

En caso que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.

En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 15 días. Caso contrario, se le podrá denegar el acceso y se deberá contactar con el jefe inmediato para solicitar al administrador de la red una nueva clave.

Proteger, en la medida de sus posibilidades, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos.

Guardar por tiempo indefinido la máxima reserva y no se debe emitir al exterior datos de carácter personal contenidos en cualquier tipo de soporte.

Utilizar el menor número de listados que contengan datos de carácter personal y mantener los mismos en lugar seguro y fuera del alcance de terceros.

Cuando entre en posesión de datos de carácter personal, se entiende que dicha posesión es estrictamente temporal, y debe devolver los soportes que contienen los datos inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos.

Los usuarios sólo podrán crear ficheros que contengan datos de carácter personal para un uso temporal y siempre necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán ubicados en unidades locales de disco de la computadora de trabajo y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.

Los usuarios deben notificar a su jefe inmediato cualquier incidencia que detecten que afecte o pueda afectar a la seguridad de los datos de carácter personal: pérdida de listados y/o dispositivos de almacenamiento, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos.

Los usuarios únicamente introducirán datos identificativos y direcciones o teléfonos de personas en las agendas de contactos de las herramientas ofimáticas.

### **3.4.3 A LAS REDES**

La Dirección de Tecnologías de la Información y Comunicación es responsable de proporcionar a los usuarios el acceso a los recursos informáticos.

La Dirección de Tecnologías de la Información y Comunicación es la responsable de difundir el reglamento para el uso de la red y de procurar su cumplimiento.

Dado el carácter unipersonal del acceso a la Red de EMELNORTE, la Dirección de Tecnologías de la Información y Comunicación verificará el uso responsable, de acuerdo con el Reglamento para el uso de la red.

El acceso lógico a equipo especializado de cómputo (servidores, enrutadores, switches, bases de datos, equipo de supercómputo centralizado y distribuido, etc.) conectado a la red es administrado por la Dirección de Tecnologías de la Información y Comunicación.

Todo el equipo de cómputo que esté o sea conectado a la Red de EMELNORTE, o aquellas que en forma autónoma se tengan y que sean propiedad de la institución, debe de sujetarse a los procedimientos de acceso que emite La Dirección de Tecnologías de la Información y Comunicación.

La Dirección de Tecnologías de la Información y Comunicación, será la responsable de cambiar periódicamente las claves de acceso a la red inalámbrica.

La Dirección de Tecnologías de la Información y Comunicación, deberá mantener respaldos de las configuraciones de servidores, enrutadores, switches, bases de datos, etc.

### **3.4.4 AL SISTEMA OPERATIVO, LAS APLICACIONES, INFORMACIÓN**

El manejo de información administrativa que se considere de uso restringido deberá ser cifrado con el objeto de garantizar su integridad.

Tendrá acceso a los sistemas administrativos solo el personal de EMELNORTE o persona que tenga la autorización por La Dirección de Tecnologías de la Información y Comunicación.

Los servidores de bases de datos administrativos son dedicados, por lo que se prohíben los accesos de cualquiera, excepto para el personal la Dirección de Tecnologías de la Información y Comunicación.

El control de acceso a cada sistema de información de EMELNORTE será determinado por la unidad responsable de generar y procesar los datos involucrados.

Toda salida de información (en soportes informáticos o por correo electrónico) sólo podrá ser realizada por personal autorizado y será necesaria la autorización formal del responsable del área del que proviene.

### **3.4.5 COMPUTACIÓN MÓVIL Y TRABAJO REMOTO**

La Dirección de Tecnologías de la Información y Comunicación es la responsable de proporcionar el servicio de acceso remoto y computación móvil, las normas de acceso a los recursos informáticos disponibles.

Para el caso especial de los recursos de cómputo a terceros deberán ser autorizados por la Dirección de Tecnologías de la Información y Comunicación.

El usuario de estos servicios deberá sujetarse al Reglamento de Uso de la Red de EMELNORTE y en concordancia con los lineamientos generales de uso de Internet.

El acceso remoto que realicen personas ajenas a la institución deberá cumplir las normas establecidas por la Dirección de Tecnologías de la Información y Comunicación.

El acceso a los servicios se realizará mediante conexiones seguras, las mismas que serán configuradas previamente por la Dirección de TIC's y asignará un usuario y contraseña para su correcto uso.

### **3.4.6 A LA WEB**

La Dirección de Tecnologías de la Información y Comunicación es la responsable de instalar y administrar el o los servidor(es) de Internet. Es decir, sólo se permiten servidores de páginas autorizados por la Dirección de Tecnologías de la Información y Comunicación.

La Dirección de Tecnologías de la Información y Comunicación deberá emitir las normas y los requerimientos para la instalación de servidores de páginas locales, de bases de datos, del uso de la Intranet institucional, así como las especificaciones para que el acceso a estos sea seguro.

Los accesos a las páginas de Web a través de los navegadores deben sujetarse a las normas que previamente se manifiestan en el Reglamento de acceso a la red de EMELNORTE.

A los responsables de los servidores de Web corresponde la verificación de respaldo y protección adecuada.

Toda la programación involucrada en la tecnología Web deberá estar de acuerdo con las normas y procedimientos establecidas por La Dirección de Tecnologías de la Información y Comunicación.

El material que aparezca en la página de Internet de EMELNORTE deberá ser aprobado para su publicación por la Presidencia Ejecutiva, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).

Con referencia a la seguridad y protección de las páginas, así como al diseño de las mismas deberá referirse a las consideraciones de diseño de páginas electrónicas establecidas por la Dirección de Tecnologías de la Información y Comunicación.

## **3.5 SOFTWARE**

Todo el personal que accede a los Sistemas de Información de EMELNORTE debe utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de utilización.

### **3.5.1 DE LA ADQUISICIÓN**

En concordancia con la política de la institución, la Dirección de Tecnologías de la Información y Comunicación es la encargada en la entidad de establecer los lineamientos para adquisición de sistemas informáticos.

En los proyectos que ejecutan las diferentes áreas de EMELNORTE deberán presupuestarse los recursos necesarios para la adquisición de sistemas de información licenciados o el desarrollo de sistemas de información a la medida.

Corresponderá a la Dirección de Tecnologías de la Información y Comunicación establecer las normas para el tipo de licenciamiento, cobertura, transferibilidad, certificación y vigencia.

La Dirección de Tecnologías de la Información y Comunicación deberá propiciar la adquisición y asesoramiento en cuanto a software de vanguardia.

### **3.5.2 DE LA INSTALACIÓN**

Corresponde a la Dirección de Tecnologías de la Información y Comunicación establecer las normas y procedimientos para la instalación y supervisión del software básico para cualquier tipo de equipo.

En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permitirá la instalación de software con licenciamiento apropiado y acorde a la propiedad intelectual.

La Dirección de Tecnologías de la Información y Comunicación es la responsable de brindar asesoría y supervisión para la instalación de software informático y de telecomunicaciones.

La instalación de software que desde el punto de vista de la Dirección de Tecnologías de la Información y Comunicación pudiera poner en riesgo los recursos de la institución no está permitida.

Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, vacunas, privilegios de acceso y otros que se apliquen).

A todo el personal tiene prohibido instalar copias ilegales de cualquier programa, incluidos los estandarizados.

El personal tiene prohibido borrar cualquiera de los programas instalados legalmente.

### **3.5.3 DE LA ACTUALIZACIÓN**

La adquisición y actualización de software para equipo especializado de cómputo y de telecomunicaciones se llevará a cabo de acuerdo con la programación que anualmente sea propuesta por la Dirección de Tecnologías de la Información y Comunicación.

Corresponde la Dirección de Tecnologías de la Información y Comunicación autorizar cualquier adquisición y actualización de software.

Las actualizaciones del software de uso común o más generalizado se llevarán a cabo de acuerdo como lo establezca la Dirección de Tecnologías de la Información y Comunicación.

### **3.5.4 DE LA AUDITORIA DE SOFTWARE INSTALADO**

El personal encargado del control interno de EMELNORTE es el responsable de realizar revisiones periódicas para asegurar que el software instalado en los computadores de la institución cuente con licencia.

### **3.5.5 DEL SOFTWARE PROPIEDAD DE LA INSTITUCIÓN**

Todos los programas de la institución sean adquiridos mediante compra, donación o cesión son de su propiedad y mantendrán los derechos que la ley de propiedad intelectual le confiera.

La Dirección de Tecnologías de la Información y Comunicación en coordinación con el procedimiento de almacenamiento, aseguramiento e inventarios deberá tener un registro de todos los paquetes de programación.

Todos los sistemas programáticos (programas, bases de datos, sistemas operativos, interfaces) desarrollados con o a través de los recursos de EMELNORTE se mantendrán como propiedad de la institución respetando la propiedad intelectual de los mismos.



Es obligación de todos los usuarios que manejen información masiva, mantener el respaldo correspondiente de la misma ya que se considera como un activo de la institución que debe preservarse.

Los datos, las bases de datos, la información generada por el personal y los recursos informáticos de la institución deben estar resguardados.

La Dirección de Tecnologías de la Información y Comunicación propiciará la gestión de patentes y derechos de creación de software de propiedad de la institución.

La Dirección de Tecnologías de la Información y Comunicación administrará los diferentes tipos de licencias de software y vigilará su vigencia en concordancia con la política informática.

### **3.5.6 DE LA PROPIEDAD INTELECTUAL**

Corresponde a la Dirección de Tecnologías de la Información y Comunicación procurar que todo el software instalado en EMELNORTE esté de acuerdo con la ley de propiedad intelectual a que dé lugar.

## **3.6 INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN**

La Dirección de Tecnologías de la Información y Comunicación busca asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.

Es conveniente establecer el reporte formal del evento y los procedimientos de escalada.

Todos los empleados, contratistas y usuarios de tercera parte deberían tener conciencia sobre los procedimientos para el reporte de los diferentes tipos de evento y las debilidades que puedan tener impacto en la seguridad de los activos de la organización.

Se les debería exigir que reporten todos los eventos de seguridad de la información y las debilidades tan pronto sea posible al punto de contacto designado.

### **3.6.1 REPORTE SOBRE LOS EVENTOS**

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

Se debería instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente que establezca la acción que se ha de tomar al recibir el reporte sobre un evento de seguridad de la información. Se debería establecer un punto de contacto para el reporte de los eventos de seguridad de la información. Es conveniente garantizar que este punto de contacto se conoce en toda la organización, siempre está disponible y puede suministrar respuesta oportuna y adecuada.

Todos los empleados, contratistas y usuarios de tercera parte deberían tener conciencia de su responsabilidad para reportar todos los eventos de seguridad de la información lo más pronto posible.

Deberían conocer el procedimiento para reportar los eventos de seguridad de la información y el punto de contacto. Los procedimientos de reporte deberían incluir los siguientes aspectos:

- a) Procesos adecuados de retroalimentación para garantizar que aquellos que reportan los eventos de seguridad de la información reciben notificación de los resultados después de que se ha tratado y solucionado el problema;
- b) Formatos para el reporte de los eventos de seguridad de la información para contener la acción de reporte y ayudar a que la persona que hace el reporte recuerde todas las acciones necesarias en caso de un evento de seguridad de la información;
- c) El comportamiento correcto en caso de un evento de seguridad de la información.

### **3.6.2 REPORTE SOBRE LAS DEBILIDADES**

Se debería exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.

Todos los empleados, contratistas y usuarios de terceras partes deberían informar sobre estos asuntos a su director o directamente a su proveedor de servicio, tan pronto sea posible para evitar los incidentes de seguridad de la información. Los mecanismos de reporte deberían ser fáciles, accesibles y disponibles. Se les debería informar a ellos que, en ninguna circunstancia, deberían intentar probar una debilidad sospechada.

### **3.6.3 GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN**

La Dirección de Tecnologías de la Información y Comunicación tiene como objetivo asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.

Es conveniente establecer las responsabilidades y los procedimientos para manejar los eventos y debilidades de la seguridad de la información de manera eficaz una vez se han reportado. Se debería aplicar un proceso de mejora continua a la respuesta para monitorear, evaluar y gestionar en su totalidad los incidentes de seguridad de la información.

Cuando se requiere evidencia, ésta se debería recolectar para garantizar el cumplimiento de los requisitos legales.

## **3.7 SUPERVISIÓN Y CUMPLIMIENTO**

### **3.7.1 CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD**

Debido al carácter confidencial de la información, el personal de la Dirección de Tecnologías de la Información y deberá de actuar de acuerdo con lo establecido en el Código de Ética, normas y procedimientos que rigen en la empresa.

Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo a las sanciones disciplinarias y penales correspondientes.

Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del servicio dependiendo de la gravedad de la falta y de la malicia o perversidad que esta manifiesta.

### **3.7.2 VERIFICACIÓN DEL CUMPLIMIENTO TÉCNICO**

Para efectos de que la institución disponga de una red con alto grado de confiabilidad, será necesario que se realice un monitoreo constante sobre todos y cada uno de los servicios que las tecnologías de la Internet e Intranet disponen.

### **3.7.3 CONSIDERACIONES DE LA AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN**

Las auditorías de cada actividad donde se involucren aspectos de seguridad lógica y física deberán realizarse periódicamente y deberá sujetarse al calendario que establezca planeación y direccionamiento estratégico.

## **CAPÍTULO IV**

### **4 CONCLUSIONES Y RECOMENDACIONES**

#### **4.1 CONCLUSIONES**

1. Es responsabilidad de los usuarios de equipos y servicios tecnológicos de EMELNORTE cumplir las políticas y normas del MANUAL DE POLÍTICAS Y NORMAS DE SEGURIDAD INFORMÁTICA.
2. La Dirección de TIC's emitirá y revisará el cumplimiento de las políticas y normas de seguridad informática que permitan realizar acciones correctivas y preventivas para el cuidado y mantenimiento de los equipos que forman parte de la infraestructura tecnológica de la empresa.
3. La organización y ejecución de pruebas, inspecciones y auditorias (internas y externas) para asegurar la continuidad de la integridad funcional del MANUAL DE POLÍTICAS Y NORMAS DE SEGURIDAD INFORMÁTICA.
4. Todas las acciones en las que se comprometa la seguridad de la empresa y que no esten previstas en este manual, deberán ser revisadas por la Dirección de TIC's para dictar una resolución sujetandose al estado de derecho y a la normativa vigente.
5. El incumplimiento a cualquiera de las políticas establecidas en el manual acarreará las sanciones de tipo disciplinario y legales a que hubiera lugar de acuerdo a la normativa vigente.

## 4.2 RECOMENDACIONES

1. Legalizar ante los estamentos jurídicos el “MANUAL DE POLÍTICAS Y NORMAS DE SEGURIDAD INFORMÁTICA”.
2. Mantener siempre actualizado el “MANUAL DE POLÍTICAS Y NORMAS DE SEGURIDAD INFORMÁTICA”.
3. Socializar con todos los empleados y trabajadores de la empresa el “MANUAL DE POLÍTICAS Y NORMAS DE SEGURIDAD INFORMÁTICA”.
4. Recomendar la elaboración de manuales de políticas y normas de todas las actividades que se realizan en el departamento de TIC's.
5. Crear un Sistema Informático de Gestión de Seguridad de la información, que supervise y normalice, toda actividad relacionada con la seguridad informática.
6. Recomendar que durante la etapa estudiantil dentro de la Universidad Técnica del Norte las materias impartidas sean teóricas y prácticas para tener un mejor desarrollo en la vida profesional.
7. Crear en la Universidad Técnica del Norte un registro con las necesidades de la comunidad para que las carreras técnicas desarrollen la mejor solución.

## BIBLIOGRAFÍA

1. Costas Santos, J. (2011). *SEGURIDAD Y ALTA DISPONIBILIDAD*. CFGS. Rama.
2. Dante Cantone, M. (2011). *ADMINISTRACION DE STORAGE Y BACKUPS*. Rama.
3. Escrivá Gascó, G., Romero Serrano, R. M., Ramada, D. J., & Onrubia Pérez, R. (2013). *SEGURIDAD INFORMÁTICA*. Macmillan Profesional.
4. Gomez Vieites, A. (2011). *ENCICLOPEDIA DE LA SEGURIDAD INFORMATICA*. Rama.
5. Gomez Vieites, A., & García Tomé, A. (2011). *GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA*. Starbook Editorial, S.A.
6. Gomez Vietes, A., & García Tomé, A. (2011). *SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS*. Starbook Editorial, S.A.
7. Instituto Ecuatoriano de Normalización. (2009). *SISTEMAS DE GESTIÓN DE LA CALIDAD. REQUISITOS*. Quito: INEN.
8. Instituto Ecuatoriano de Normalización. (2009). *TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE LA SEGURIDAD - CÓDIGO DE PRÁCTICA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN*. Quito: INEN.
9. Instituto Ecuatoriano de Normalización. (2011). *TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE SEGURIDAD - SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) - REQUISITOS*. Quito: INEN.
10. Lacasta, R., Sanmartí, E., & Velasco, J.
11. Merino Bada, C., & Cañizares Sales, R. (2011). *IMPLANTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN*. Fundación Confemetal.

12. Purificación, A. (2010). *SEGURIDAD INFORMÁTICA. Nivel: formación profesional*. Ra-ma.
13. Scrib. (2009). *Seguridad de la información. Tipos de ataques Informáticos*. Recuperado el 9 de Julio de 2013, de Scrib: <http://www.scribd.com/doc/19397003/Tipos-de-Ataques-informaticos>
14. Vallecilla Mosquera, J. (2009). *Seguridad de las TIC bajo protocolos TCP/IP*. Recuperado el 9 de Julio de 2013, de Vallecilla Mosquera, Juan: <http://biblioteca.cenace.org.ec:8180/jspui/handle/123456789/86>
15. Vieites Gomez, A., & García Tomé, A. (2011). *AUDITORÍA DE SEGURIDAD INFORMÁTICA*. Starbook Editorial, S.A.



# ANEXOS

## MANUAL DE POLÍTICAS DE SEGURIDAD EMELNORTE

Este manual de políticas de seguridad es elaborado de acuerdo al análisis de riesgos y vulnerabilidades en las direcciones de la Empresa Eléctrica Regional Norte S.A. – EMELNORTE, por consiguiente el alcance de estas políticas, se encuentra sujeto a la empresa.

### 1 ACTIVOS

Toda adquisición de tecnología informática se efectuará a través del Departamento de Adquisiciones (Portal de Compras Públicas) previo a un requerimiento de usuario y la respectiva autorización del Director correspondiente, deberá constar en el presupuesto.

La adquisición de bienes informáticos, quedará sujeta a los lineamientos establecidos en esta política.

#### 1.1 DE INFORMACIÓN

La Dirección de Tecnologías de la Información y Comunicación tiene como objetivo asegurar que la información recibe el nivel de protección adecuado. La información se debería clasificar para indicar la necesidad, las prioridades y el grado esperado de protección al manejar la información.

La información tiene diferentes grados de sensibilidad e importancia. Algunos elementos pueden requerir un grado adicional de protección o manejo especial. Se recomienda utilizar un esquema de clasificación de la información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas especiales de manejo.

La información que cada usuario mantiene en sus equipos es de su responsabilidad, la Dirección de Tecnologías de la Información y Comunicación, no se responsabilizará en caso de pérdida de la misma.

## **1.2 DE SOFTWARE, FÍSICOS Y SERVICIOS**

La Dirección de Tecnologías de la Información y Comunicación, al planear las operaciones relativas a la adquisición de bienes informáticos y/o servicios, establecerá prioridades y en su selección deberá tomar en cuenta: estudio técnico, precio, calidad, experiencia, desarrollo tecnológico, estándares y capacidad, entendiéndose por:

### **Precio**

Costo inicial, costo de mantenimiento y consumibles por el período estimado de uso de los equipos;

### **Calidad**

Parámetro cualitativo que especifica las características técnicas de los recursos informáticos.

### **Experiencia**

Presencia en el mercado nacional e internacional, estructura de servicio, la confiabilidad de los bienes y certificados de calidad con los que se cuente.

### **Desarrollo Tecnológico**

Se deberá analizar su vida útil, su nivel tecnológico con respecto a la oferta existente y su permanencia en el mercado.

### **Capacidades**

Se deberá analizar si satisface la demanda actual con un margen de holgura y capacidad de crecimiento para soportar la carga de trabajo del área.

Los Recursos Informáticos, Datos, Software, Red Corporativa y Sistemas de Comunicación Electrónica están disponibles exclusivamente para cumplir las obligaciones y propósito de la operación para la que fueron diseñados e implantados.

Todos los usuarios de dichos recursos deben saber que no tiene el derecho de confidencialidad en su uso.

El introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, inmorales u ofensivos, será motivo de sanción para los funcionarios, de acuerdo a la normativa vigente.

Perturbar el trabajo de los demás enviando mensajes o archivos que puedan inferir en el trabajo de otro usuario de la red, incurrirá en la aplicación de la sanción según la normativa vigente.

El diseminar “virus”, “gusanos”, “troyanos” y otros tipos de programas dañinos para los sistemas de procesos de la información, será motivo de sanción.

## **2 EQUIPOS DE CÓMPUTO**

### **2.1 DE LA INSTALACIÓN**

La instalación del equipo de cómputo, quedará sujeta a los siguientes lineamientos:

Los equipos para uso interno se instalarán en lugares adecuados, lejos de polvo y alto tráfico de personas.

Todo equipo de cómputo, que esté o sea conectado a la red de EMELNORTE, o aquel que en forma autónoma se tenga y que sea propiedad de la institución debe sujetarse a las normas y procedimientos de instalación que emite La Dirección de Tecnologías de la Información y Comunicación.

La Dirección de TIC's deberá contar con un plano actualizado de las instalaciones eléctricas y de comunicaciones.

Las instalaciones eléctricas y de comunicaciones, estarán de preferencias fijas o en su defecto resguardadas del paso de personas o máquinas, y libres de cualquier interferencia eléctrica o magnética.

Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.

En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.

Los equipos informáticos mantendrán una estandarización en los nombres que se le asigne, cumpliendo con las necesidades de la Dirección de TIC's. El nombre no debe exceder de 15 caracteres.

El formato de nombres de los equipos de cómputo (computadores de escritorio, portátiles) sería el siguiente:

10IBATICSOP-16

10: ÁREA REFERENCIAL CÓDIGO PROVINCIAL

IBA: CIUDAD, CANTÓN DE UBICACIÓN DE LA EMPRESA O SUCURSAL

TIC: CORRESPONDE A LA DIRECCIÓN

SOP: ÁREA DE LA DIRECCIÓN

16: CUARTO OCTETO DE LA DIRECCIÓN IP

Para el caso de impresoras será el siguiente formato indicado:

10IBATICIMP-24

10: ÁREA REFERENCIAL CÓDIGO PROVINCIAL

IBA: CIUDAD, CANTÓN DE UBICACIÓN DE LA EMPRESA O SUCURSAL

TIC: CORRESPONDE A LA DIRECCIÓN, AREA O DEPARTAMENTO

IMP: INDICA QUE ES UNA IMPRESORA

24: CUARTO OCTETO DE LA DIRECCIÓN IP

Para el caso de cámaras de video vigilancia será el siguiente:

IBMATPB20-51

IBA: CIUDAD, CANTÓN DE UBICACIÓN DE LA EMPRESA O SUCURSAL

MAT: NOMBRE DE LA SUCURSAL

PB: UBICACIÓN FISICA

20: CUARTO OCTETO DE LA DIRECCIÓN IP

51: VLAN ASIGNADA

Los formatos para los nombres de los equipos informáticos debe actualizarse periódicamente por la Dirección de TIC's.

## **2.2 PARA EL MANTENIMIENTO**

Es obligación de la Dirección de TIC's vigilar que el equipo de cómputo se use bajo las condiciones especificadas por el proveedor y de acuerdo a las funciones del área a la que se asigne.

Los empleados de la empresa al usar el equipo de cómputo, se abstendrán de consumir alimentos, fumar o realizar actos que perjudiquen el funcionamiento del mismo o deterioren la información almacenada en medios magnéticos, ópticos, o medios de almacenamiento removibles de última generación.

A la Dirección de TIC's corresponde la realización del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física y su acondicionamiento específico a que tenga lugar. Para tal fin debe emitir las normas y procedimientos respectivos.

Los responsables la Dirección de Tecnologías de la Información y Comunicación son los únicos autorizados para realizar mantenimiento preventivo y correctivo, o para autorizar el mantenimiento por parte de terceros.

## **2.3 DE LA ACTUALIZACIÓN**

La Dirección de TIC's es responsable de mantener versiones actualizadas de los sistemas usados en EMELNORTE, para ello se realizará un plan adecuado y a tiempo de las actualizaciones respectivas.

Todo equipo de cómputo (computadoras personales, estaciones de trabajo, supercomputadora y demás relacionados) y los de telecomunicaciones que sean propiedad de la empresa debe procurarse sean actualizados tendiendo a conservar e incrementar la calidad del servicio que presta, mediante la mejora sustantiva de su desempeño.

## **2.4 DE LA RE-UBICACIÓN**

La reubicación de los equipos de cómputo se realizará satisfaciendo las normas y procedimientos que para ello emita la Dirección de Tecnologías de la Información y Comunicación.

En caso de existir personal técnico de apoyo, este notificará de los cambios tanto físicos como de software que realice la Dirección de Tecnologías de la Información y Comunicación y al procedimiento de ALMACENAMIENTO, ASEGURAMIENTO E INVENTARIOS notificando también los cambios de los equipos para adjuntarlos al inventario.

El equipo de cómputo a reubicar se hará únicamente bajo la autorización del responsable, contando el lugar a donde se hará la ubicación con los medios necesarios para la instalación del equipo.

Es responsabilidad de cada usuario informar a la Dirección de TIC's, mediante hojas de requerimiento la necesidad de reubicar los equipos para dar la asistencia correspondiente.

## **2.5 DE LA SEGURIDAD**

Cada usuario es responsable de mantener sus claves de seguridad en secreto.

Los equipos de la Empresa sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.

Cualquier falla en los computadores o en la red debe reportarse inmediatamente a la Dirección de Tecnologías de la Información y Comunicación para lograr evitar problemas serios como pérdida de la información o indisponibilidad de los servicios.

No deben usarse dispositivos de almacenamiento en cualquier computadora de la Empresa sin que previamente se haya verificado que están libres de cualquier tipo de virus.

Los usuarios de PCs son responsables de realizar periódicamente el respaldo de los datos guardados en sus PCs, para evitar pérdidas de información.

Los usuarios de PCs son responsables de proteger los programas y datos contra pérdida o daño.

El personal que utiliza un computador portátil que contenga información confidencial de la Empresa, debe protegerlo y evitar el acceso a la información de personas no autorizadas.

Para prevenir el acceso no autorizado, utilice contraseñas difíciles de predecir y además debe configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además, cada vez que deba ausentarse de su oficina debe activar el protector de pantalla manualmente.

Para prevenir el ataque de virus, no está permitido el uso de módems de internet de cualquier operadora en los equipos de EMELNORTE que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la red interna de la Empresa.

Debe respetarse y no modificar la configuración de hardware y software establecida por la Dirección de Tecnologías de la Información y Comunicación.

Está terminantemente prohibido hacer copias o usar software de EMELNORTE para fines personales.

Los usuarios no deben copiar a un dispositivo de almacenamiento externo, el software de las computadoras de la Empresa, sin la aprobación previa de la Dirección de Tecnologías de la Información y Comunicación.

No debe utilizarse software descargado de Internet o software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por la Dirección de Tecnologías de la Información y Comunicación.

Se prohíbe estrictamente la instalación de software no autorizado, sin que haya sido previamente aprobado por la Dirección de Tecnologías de la Información y Comunicación, con el fin de prevenir la introducción de virus informáticos.

El internet es estrictamente para uso de las actividades propias de la Empresa y su uso será autorizado por la Presidencia Ejecutiva.

Queda totalmente prohibido, sacar los equipos de computación de la Empresa sin previa autorización por parte del director de cada dependencia. En caso de ser necesario sacar los mismos, se debe llenar el formulario de movilización de equipos y entregar al personal de seguridad.

### **3 COMUNICACIONES Y OPERACIONES**

#### **3.1 PROCEDIMIENTOS Y RESPONSABILIDADES**

El objetivo de la Dirección de Tecnologías de la Información y Comunicación es asegurar la operación correcta y segura de los servicios de procesamiento de información.

Se deberían establecer todas las responsabilidades y los procedimientos para la gestión y operación de todos los servicios de procesamiento de información. Esto incluye el desarrollo de procedimientos operativos apropiados.

Cuando sea conveniente, se debería implementar la separación de funciones para reducir el riesgo de uso inadecuado deliberado o negligente del sistema.

#### **3.2 PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA**

La Dirección de Tecnologías de la Información y Comunicación pretende minimizar el riesgo de fallas en los sistemas.



Se requieren una previa planificación y preparación para garantizar la disponibilidad de la capacidad y los recursos adecuados para entregar el desempeño requerido del sistema.

Es necesario hacer proyecciones de la capacidad futura para reducir el riesgo de sobrecarga del sistema.

Los requisitos operativos de los sistemas nuevos se deberían establecer, documentar y probar antes de su aceptación y uso.

### **3.3 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS Y MÓVILES**

La Dirección de Tecnologías de la Información y Comunicación busca proteger la integridad del software y de la información.

Se requieren precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no autorizados.

El software y los servicios de procesamiento de información son vulnerables a la introducción de códigos maliciosos tales como virus de computador, gusanos en la red, caballos troyanos y bombas lógicas. Los usuarios deberían ser conscientes de los peligros de los códigos maliciosos. Los directores deberían, cuando sea apropiado, coordinar con la dirección de TIC's los controles para evitar, detectar y retirar los códigos maliciosos y controlar los códigos móviles.

Se encuentra prohibida la conexión de equipos móviles, que no sean de la empresa, a la red interna de EMELNORTE, a menos de que exista la respectiva autorización de la Presidencia Ejecutiva.

### **3.4 RESPALDO**

La Dirección de Tecnologías de la Información y Comunicación pretende mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.

Se deberían establecer procedimientos de rutina para implementar la política y la estrategia de respaldo acordada para hacer copias de la seguridad de los datos y probar sus tiempos de restauración.

El personal responsable de mantener los servicios informáticos operativos, deberá sacar respaldos de la información de forma mensual y almacenarlos en un lugar seguro.

### **3.5 SEGURIDAD EN LAS REDES**

La Dirección de Tecnologías de la Información y Comunicación busca asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

La gestión segura de las redes, las cuales pueden sobrepasar las fronteras de la organización, exige la consideración cuidadosa del flujo de datos, las implicaciones legales, el monitoreo y la protección.

También pueden ser necesarios los controles adicionales para proteger la información sensible que pasa por las redes públicas.

### **3.6 MANEJO DE LOS MEDIOS**

La Dirección de Tecnologías de la Información y Comunicación trata de evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del negocio.

Estos medios se deberían controlar y proteger de forma física.

Se deberían establecer procedimientos operativos adecuados para proteger documentos, medios de computador (por ejemplo cintas, discos), datos de entrada/salida y documentación del sistema contra divulgación, modificación, remoción y destrucción no autorizadas.

### **3.7 MONITOREO**

La Dirección de Tecnologías de la Información y Comunicación pretende detectar actividades de procesamiento de la información no autorizadas.

Se deberían monitorear los sistemas y registrar los eventos de la seguridad de la información. Los registros de operador y la actividad de registro de fallas se deberían utilizar para garantizar la identificación de los problemas del sistema de información.

Una organización debería cumplir todos los requisitos legales pertinentes que se aplican a sus actividades de monitoreo y registro.

Debería emplearse el monitoreo del sistema para verificar la eficacia de los controles adoptados y revisar el cumplimiento de un modelo de política de acceso.

## **4 CONTROL DE ACCESO**

### **4.1 GESTIÓN DEL ACCESO DE LOS USUARIOS**

Todos los usuarios con acceso a un sistema de información o a una red informática, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.

Ningún usuario recibirá un identificador de acceso a la Red de Comunicaciones, Recursos Informáticos o Aplicaciones hasta que no acepte formalmente la Política de Seguridad vigente.

Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por el responsable de la información.

La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.

Los identificadores para usuarios temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.

Cada usuario, dispondrá de un identificador único, el cual se corresponde con la cuenta de usuario.

A cada identificador de usuario corresponderá una, y solo una persona física.

Todas aquellas operaciones realizadas por un usuario, serán siempre atribuidas al identificador utilizado que se hubiere identificado ante el sistema de información.

La Dirección de TIC's, realizará mensualmente, la actualización de usuarios, en coordinación con la Dirección de Talento Humano.

## **4.2 RESPONSABILIDAD DE LOS USUARIOS**

Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.

Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.

Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.

Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar a su jefe inmediato y éste reportar al responsable de la administración de la red.

El Usuario debe utilizar una contraseña compuesta por un mínimo de ocho caracteres constituida por una combinación de caracteres alfabéticos, numéricos y especiales.

La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos.

En caso que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.

En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 15 días. Caso contrario, se le podrá denegar el acceso y se deberá contactar con el jefe inmediato para solicitar al administrador de la red una nueva clave.

Proteger, en la medida de sus posibilidades, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos.

Guardar por tiempo indefinido la máxima reserva y no se debe emitir al exterior datos de carácter personal contenidos en cualquier tipo de soporte.

Utilizar el menor número de listados que contengan datos de carácter personal y mantener los mismos en lugar seguro y fuera del alcance de terceros.

Cuando entre en posesión de datos de carácter personal, se entiende que dicha posesión es estrictamente temporal, y debe devolver los soportes que contienen los datos inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos.

Los usuarios sólo podrán crear ficheros que contengan datos de carácter personal para un uso temporal y siempre necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán ubicados en unidades locales de disco de la computadora de trabajo y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.

Los usuarios deben notificar a su jefe inmediato cualquier incidencia que detecten que afecte o pueda afectar a la seguridad de los datos de carácter personal: pérdida de listados y/o dispositivos de almacenamiento, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos.

Los usuarios únicamente introducirán datos identificativos y direcciones o teléfonos de personas en las agendas de contactos de las herramientas ofimáticas.

### **4.3 A LAS REDES**

La Dirección de Tecnologías de la Información y Comunicación es responsable de proporcionar a los usuarios el acceso a los recursos informáticos.

La Dirección de Tecnologías de la Información y Comunicación es la responsable de difundir el reglamento para el uso de la red y de procurar su cumplimiento.

Dado el carácter unipersonal del acceso a la Red de EMELNORTE, la Dirección de Tecnologías de la Información y Comunicación verificará el uso responsable, de acuerdo con el Reglamento para el uso de la red.

El acceso lógico a equipo especializado de cómputo (servidores, enrutadores, switches, bases de datos, equipo de supercómputo centralizado y distribuido, etc.) conectado a la red es administrado por la Dirección de Tecnologías de la Información y Comunicación.

Todo el equipo de cómputo que esté o sea conectado a la Red de EMELNORTE, o aquellas que en forma autónoma se tengan y que sean propiedad de la institución, debe de sujetarse a los procedimientos de acceso que emite La Dirección de Tecnologías de la Información y Comunicación.

La Dirección de Tecnologías de la Información y Comunicación, será la responsable de cambiar periódicamente las claves de acceso a la red inalámbrica.

La Dirección de Tecnologías de la Información y Comunicación, deberá mantener respaldos de las configuraciones de servidores, enrutadores, switches, bases de datos, etc.

### **4.4 AL SISTEMA OPERATIVO, LAS APLICACIONES, INFORMACIÓN**

El manejo de información administrativa que se considere de uso restringido deberá ser cifrado con el objeto de garantizar su integridad.

Tendrá acceso a los sistemas administrativos solo el personal de EMELNORTE o persona que tenga la autorización por La Dirección de Tecnologías de la Información y Comunicación.

Los servidores de bases de datos administrativos son dedicados, por lo que se prohíben los accesos de cualquiera, excepto para el personal la Dirección de Tecnologías de la Información y Comunicación.

El control de acceso a cada sistema de información de EMELNORTE será determinado por la unidad responsable de generar y procesar los datos involucrados.

Toda salida de información (en soportes informáticos o por correo electrónico) sólo podrá ser realizada por personal autorizado y será necesaria la autorización formal del responsable del área del que proviene.

#### **4.5 COMPUTACIÓN MÓVIL Y TRABAJO REMOTO**

La Dirección de Tecnologías de la Información y Comunicación es la responsable de proporcionar el servicio de acceso remoto y computación móvil, las normas de acceso a los recursos informáticos disponibles.

Para el caso especial de los recursos de cómputo a terceros deberán ser autorizados por la Dirección de Tecnologías de la Información y Comunicación.

El usuario de estos servicios deberá sujetarse al Reglamento de Uso de la Red de EMELNORTE y en concordancia con los lineamientos generales de uso de Internet.

El acceso remoto que realicen personas ajenas a la institución deberá cumplir las normas establecidas por la Dirección de Tecnologías de la Información y Comunicación.

El acceso a los servicios se realizará mediante conexiones seguras, las mismas que serán configuradas previamente por la Dirección de TIC's y asignará un usuario y contraseña para su correcto uso.

#### **4.6 A LA WEB**

La Dirección de Tecnologías de la Información y Comunicación es la responsable de instalar y administrar el o los servidor(es) de Internet. Es decir, sólo se permiten servidores de páginas autorizados por la Dirección de Tecnologías de la Información y Comunicación.

La Dirección de Tecnologías de la Información y Comunicación deberá emitir las normas y los requerimientos para la instalación de servidores de páginas locales, de bases de datos, del uso de la Intranet institucional, así como las especificaciones para que el acceso a estos sea seguro.

Los accesos a las páginas de Web a través de los navegadores deben sujetarse a las normas que previamente se manifiestan en el Reglamento de acceso a la red de EMELNORTE.

A los responsables de los servidores de Web corresponde la verificación de respaldo y protección adecuada.

Toda la programación involucrada en la tecnología Web deberá estar de acuerdo con las normas y procedimientos establecidas por La Dirección de Tecnologías de la Información y Comunicación.

El material que aparezca en la página de Internet de EMELNORTE deberá ser aprobado para su publicación por la Presidencia Ejecutiva, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).

Con referencia a la seguridad y protección de las páginas, así como al diseño de las mismas deberá referirse a las consideraciones de diseño de páginas electrónicas establecidas por la Dirección de Tecnologías de la Información y Comunicación.

## **5 SOFTWARE**

Todo el personal que accede a los Sistemas de Información de EMELNORTE debe utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de utilización.

### **5.1 DE LA ADQUISICIÓN**

En concordancia con la política de la institución, la Dirección de Tecnologías de la Información y Comunicación es la encargada en la entidad de establecer los lineamientos para adquisición de sistemas informáticos.



En los proyectos que ejecutan las diferentes áreas de EMELNORTE deberán presupuestarse los recursos necesarios para la adquisición de sistemas de información licenciados o el desarrollo de sistemas de información a la medida.

Corresponderá a la Dirección de Tecnologías de la Información y Comunicación establecer las normas para el tipo de licenciamiento, cobertura, transferibilidad, certificación y vigencia.

La Dirección de Tecnologías de la Información y Comunicación deberá propiciar la adquisición y asesoramiento en cuanto a software de vanguardia.

## **5.2 DE LA INSTALACIÓN**

Corresponde a la Dirección de Tecnologías de la Información y Comunicación establecer las normas y procedimientos para la instalación y supervisión del software básico para cualquier tipo de equipo.

En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permitirá la instalación de software con licenciamiento apropiado y acorde a la propiedad intelectual.

La Dirección de Tecnologías de la Información y Comunicación es la responsable de brindar asesoría y supervisión para la instalación de software informático y de telecomunicaciones.

La instalación de software que desde el punto de vista de la Dirección de Tecnologías de la Información y Comunicación pudiera poner en riesgo los recursos de la institución no está permitida.

Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, vacunas, privilegios de acceso y otros que se apliquen).

A todo el personal tiene prohibido instalar copias ilegales de cualquier programa, incluidos los estandarizados.

El personal tiene prohibido borrar cualquiera de los programas instalados legalmente.

### **5.3 DE LA ACTUALIZACIÓN**

La adquisición y actualización de software para equipo especializado de cómputo y de telecomunicaciones se llevará a cabo de acuerdo con la programación que anualmente sea propuesta por la Dirección de Tecnologías de la Información y Comunicación.

Corresponde la Dirección de Tecnologías de la Información y Comunicación autorizar cualquier adquisición y actualización de software.

Las actualizaciones del software de uso común o más generalizado se llevarán a cabo de acuerdo como lo establezca la Dirección de Tecnologías de la Información y Comunicación.

### **5.4 DE LA AUDITORIA DE SOFTWARE INSTALADO**

El personal encargado del control interno de EMELNORTE es el responsable de realizar revisiones periódicas para asegurar que el software instalado en los computadores de la institución cuente con licencia.

### **5.5 DEL SOFTWARE PROPIEDAD DE LA INSTITUCIÓN**

Todos los programas de la institución sean adquiridos mediante compra, donación o cesión son de su propiedad y mantendrán los derechos que la ley de propiedad intelectual le confiera.

La Dirección de Tecnologías de la Información y Comunicación en coordinación con el procedimiento de almacenamiento, aseguramiento e inventarios deberá tener un registro de todos los paquetes de programación.

Todos los sistemas programáticos (programas, bases de datos, sistemas operativos, interfaces) desarrollados con o a través de los recursos de EMELNORTE se mantendrán como propiedad de la institución respetando la propiedad intelectual de los mismos.

Es obligación de todos los usuarios que manejen información masiva, mantener el respaldo correspondiente de la misma ya que se considera como un activo de la institución que debe preservarse.

Los datos, las bases de datos, la información generada por el personal y los recursos informáticos de la institución deben estar resguardados.

La Dirección de Tecnologías de la Información y Comunicación propiciará la gestión de patentes y derechos de creación de software de propiedad de la institución.

La Dirección de Tecnologías de la Información y Comunicación administrará los diferentes tipos de licencias de software y vigilará su vigencia en concordancia con la política informática.

## **5.6 DE LA PROPIEDAD INTELECTUAL**

Corresponde a la Dirección de Tecnologías de la Información y Comunicación procurar que todo el software instalado en EMELNORTE esté de acuerdo con la ley de propiedad intelectual a que dé lugar.

## **6 INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN**

La Dirección de Tecnologías de la Información y Comunicación busca asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.

Es conveniente establecer el reporte formal del evento y los procedimientos de escalada.

Todos los empleados, contratistas y usuarios de tercera parte deberían tener conciencia sobre los procedimientos para el reporte de los diferentes tipos de evento y las debilidades que puedan tener impacto en la seguridad de los activos de la organización.

Se les debería exigir que reporten todos los eventos de seguridad de la información y las debilidades tan pronto sea posible al punto de contacto designado.

## **6.1 REPORTE SOBRE LOS EVENTOS**

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

Se debería instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente que establezca la acción que se ha de tomar al recibir el reporte sobre un evento de seguridad de la información. Se debería establecer un punto de contacto para el reporte de los eventos de seguridad de la información. Es conveniente garantizar que este punto de contacto se conoce en toda la organización, siempre está disponible y puede suministrar respuesta oportuna y adecuada.

Todos los empleados, contratistas y usuarios de tercera parte deberían tener conciencia de su responsabilidad para reportar todos los eventos de seguridad de la información lo más pronto posible.

Deberían conocer el procedimiento para reportar los eventos de seguridad de la información y el punto de contacto. Los procedimientos de reporte deberían incluir los siguientes aspectos:

- a) Procesos adecuados de retroalimentación para garantizar que aquellos que reportan los eventos de seguridad de la información reciben notificación de los resultados después de que se ha tratado y solucionado el problema;
- b) Formatos para el reporte de los eventos de seguridad de la información para contener la acción de reporte y ayudar a que la persona que hace el reporte recuerde todas las acciones necesarias en caso de un evento de seguridad de la información;
- c) El comportamiento correcto en caso de un evento de seguridad de la información.

## **6.2 REPORTE SOBRE LAS DEBILIDADES**

Se debería exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.

Todos los empleados, contratistas y usuarios de terceras partes deberían informar sobre estos asuntos a su director o directamente a su proveedor de servicio, tan pronto sea posible para evitar los incidentes de seguridad de la información. Los mecanismos de reporte deberían ser fáciles, accesibles y disponibles. Se les debería informar a ellos que, en ninguna circunstancia, deberían intentar probar una debilidad sospechada.

### **6.3 GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN**

La Dirección de Tecnologías de la Información y Comunicación tiene como objetivo asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.

Es conveniente establecer las responsabilidades y los procedimientos para manejar los eventos y debilidades de la seguridad de la información de manera eficaz una vez se han reportado. Se debería aplicar un proceso de mejora continua a la respuesta para monitorear, evaluar y gestionar en su totalidad los incidentes de seguridad de la información.

Cuando se requiere evidencia, ésta se debería recolectar para garantizar el cumplimiento de los requisitos legales.

## **7 SUPERVISIÓN Y CUMPLIMIENTO**

### **7.1 CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD**

Debido al carácter confidencial de la información, el personal de la Dirección de Tecnologías de la Información y deberá de actuar de acuerdo con lo establecido en el Código de Ética, normas y procedimientos que rigen en la empresa.

Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo a las sanciones disciplinarias y penales correspondientes.

Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del servicio dependiendo de la gravedad de la falta y de la malicia o perversidad que esta manifiesta.

## **7.2 VERIFICACIÓN DEL CUMPLIMIENTO TÉCNICO**

Para efectos de que la institución disponga de una red con alto grado de confiabilidad, será necesario que se realice un monitoreo constante sobre todos y cada uno de los servicios que las tecnologías de la Internet e Intranet disponen.

## **7.3 CONSIDERACIONES DE LA AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN**

Las auditorías de cada actividad donde se involucren aspectos de seguridad lógica y física deberán realizarse periódicamente y deberá sujetarse al calendario que establezca planeación y direccionamiento estratégico.