SEGURIDAD DE INFORMACIÓN CORPORATIVA

Memorando Nro. CELEC-EP-2015-0128-MEM

Cuenca, 22 de enero de 2015

PARA: Sr. Ing. Carlos Julio Balda Santos
Gerente CELEC EP - ELECTROGUAYAS

Cristobal Punina Lozano
Gerente CELEC EP - HIDRONACIÓN

Sr. Ing. Geovanny Pardo Salazar
Gerente CELEC EP - TRANSELECTRIC

Sr. Ing. Juan Carlos López Benalcazar
Gerente CELEC EP - TERMOPICHINCHA

Sr. Mgs. Manuel Steven Canales Gomez
Gerente CELEC EP - TERMOGAS MACHALA

Sr. Ing. Nelson Mauricio Caicedo Villota
Gerente CELEC EP - HIDROAGOYAN

Paúl Urgilés Buestán
Gerente CELEC EP - HIDROAZOGUES

Sr. Ing. Santiago Arias Hugo
Gerente CELEC EP- ENERJUBONES

Sr. Ing. Tito Quiruba Torres Sarmiento
Gerente CELEC EP - HIDROPAUTE

Sr. Ing. Victor Hugo Jácome Sánchez
Gerente CELEC EP - ENERNORTE

Sr. Ing. Wilver Alberto Cruz Zambrano
Gerente CELEC EP - TERMOESMERALDAS

Sr. Ing. Richard Edgar Vera Velez
Gerente CELEC EP - GENSUR

Sr. Ing. Rodrigo Patricio Ayala Egas
Gerente CELEC EP - HIDROTOAPI (E)

Edgar Gustavo Tamayo Jaramillo
Director Jurídico

Memorando Nro. CELEC-EP-2015-0128-MEM

Cuenca, 22 de enero de 2015

Modesto Enrique Salgado Rodriguez
Director de Generación

Patricio Gonzalo Freire Sosa
Director Administrativo Financiero

Santiago Roberto Carrillo Calderón
Director Gestión Estratégica

Segundo Vicente Barrera González
Director de Planificación de la Expansión

Sr. Ing. Raimundo Guillermo Ycaza Molina
Director de Auditoria Interna

ASUNTO: Conocimiento y Aplicación de Normas Técnicas de Seguridad de Información

En concordancia con Plan Estratégico de la Corporación y el Programa de Seguridad de Información para la Corporación, se elaboraron las Normas Técnicas de Seguridad de Información y Guías, mismas que fueron aprobadas por esta Gerencia.

Estos documentos consideran la Normativa Legal existente, las Normas Internacionasles ISO 27000, la Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27000, los estándares NERC-CIP y la Base para Protección de Infraestructura Crítica del Instituto Nacional de Normas de los Estados Unidos de América (NIST por sus siglas en inglés); con lo cual la documentación presentada, se ha enriquecido de las buenas prácticas a nivel nacional e internacional.

Los documentos que comprenden este Marco Técnico y Normativo son:

- Normas Técnicas de Seguridad de Información (SIC-NTE-001-2014)
- Guías de:

- Control de acceso SIC-GCA-001-2014
- Contratos y compromiso de confidencialidad SIC-GLG-001-2014
- Guía rápida para usuarios SIC-GLG-002-2014
- Gestión de activos de información SIC-GAI-001-2014
- Gestión del cambio cultural SIC-RH-001-2014
- Gestión de incidentes de seguridad de información SIC-GIS-001-2014
- Adquisición, desarrollo y mantenimiento de sistemas de Información

Memorando Nro. CELEC-EP-2015-0128-MEM

Cuenca, 22 de enero de 2015

SIC-ADM-001-2014

Para la aplicación del Marco Técnico y Normativo, se creó un Instructivo (SIC-INS-001-2014), en el cual se establece la programación de revisiones de cumplimiento y definiciones generales de la forma de trabajo.

Por lo anteriormente expuesto; solicito a Usted, se difundan los documentos a los servidores de su Unidad de Negocio y Dirección, para su conocimiento y aplicación.

Atentamente,

Documento firmado electrónicamente

Eduardo Barredo Heinert
GERENTE GENERAL CELEC EP

Anexos:
- Norma Técnica de Seguridad de Información
- Guía rápida para usuarios
- Guía de control de acceso
- Guía de adquisición desarrollo y mantenimiento de SI
- Guía de gestión de incidentes de seguridad de información
- Guía de gestíon de activos de información
- Guía de gestión del cambio cultural
- Guía de contratos y compromiso de confidencialidad
- Instructivo de aplicación
- RESOLUCION DESIGNACIÓN OFICIAL DE SEGURIDAD.

mica

EMPRESA PÚBLICA ESTRATÉGICA
CORPORACIÓN ELÉCTRICA DEL ECUADOR CELEC EP

RESOLUCIÓN No. CELEC EP-GGE-0026-14

DESIGNACIÓN DE OFICIAL DE SEGURIDAD DE INFORMACIÓN, AL INGENIERO FERNANDO GUERRERO B.

Ing. Eduardo Barredo Heinert
GERENTE GENERAL

CONSIDERANDO:

Que, como parte de la Estrategia Corporativa y del aseguramiento de los activos críticos de infraestructura eléctrica de la Empresa Pública Estratégica Corporación Eléctrica del Ecuador CELEC EP, la Dirección de Gestión Estratégica presentó a la Gerencia el Programa de Seguridad de Información Corporativo, preparado por el Ingeniero Fernando Guerrero B., especialista en esta disciplina.

Que, el proceso de Contratación de Consultoría para la "Evaluación, Diseño y Fiscalización de la implementación de la Seguridad de Información Corporativa" se encuentra en etapa de revisión, debido a que existen nuevos requerimientos en la Corporación que incluyen al núcleo de negocio de CNEL y CENACE.

Que, el 25 de septiembre del 2013, mediante Acuerdo Ministerial No. 166, la Secretaria Nacional de la Administración Pública dispuso a las Entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, se establece que: *"Las Entidades designarán, al interior de su institución, un Comité de Seguridad de la Información liderado con un Oficial de Seguridad de la Información, conforme lo establece el EGSI y cuya designación deberá ser comunicada a la Secretaria Nacional de la Administración Pública, en el transcurso de treinta (30) días posteriores a la emisión del presente Acuerdo"; y que, "* los Oficiales de Seguridad de la Información de los Comités de Gestión de Seguridad de la Información designados por las Instituciones, actuarán como contrapartes de la SNAP en la implementación del EGSI y en la gestión de incidentes de seguridad de la información."

Que, sobre la base de lo expuesto, el Director de Gestión Estratégica, Ing. Roberto Carrillo, mediante Memorando No. CELEC EP-MAT-DGE-0149-14, sugiere que el Ingeniero Fernando Guerrero B., funcionario de esa Dirección, sea designado como "Oficial de Seguridad de Información", quien estará a cargo entre otras funciones de:

> *Definir procedimientos para el control de los procesos operativos, los sistemas e instalaciones, y verificar su cumplimiento de manera que no afecten a la seguridad de la información,*
> *Desarrollar procedimientos adecuados de concienciación de usuarios en materia de seguridad, controles de acceso a los sistemas y administración de cambios,*
> *Coordinar todas las actividades relativas a la Seguridad de Información en la Corporación.*

Coordinar la gestión de eventos de seguridad con otras entidades gubernamentales
Otras que por naturaleza de las actividades de gestión de la seguridad de la información deban ser realizadas.

Que, de acuerdo a lo establecido en el Artículo 11 de la Ley Orgánica de Empresas Públicas, el Gerente General es responsable de la administración y gestión de la Empresa Pública y la faculta a nombrar, contratar y sustituir al talento humano.

RESUELVE:

Art. 1.- Sobre la base de lo expuesto, la Gerencia General designa a partir de la presente fecha, al ***Ing. Fernando Guerrero B.***, funcionario de la Empresa Pública en la Dirección de Gestión Estratégica de CELEC EP-Matriz, como Oficial de Seguridad de Información de esta Corporación.

Art. 2.- Disponer a la Dirección Administrativa-Financiera de CELEC EP, notificar al interesado y a la Secretaria Nacional de la Administración Pública, del particular.

Cuenca, a 17 de febrero de 2014.

Ing. Eduardo Barredo Heinert
GERENTE GENERAL
EMPRESA PÚBLICA ESTRATÉGICA
CORPORACIÓN ELÉCTRICA DEL ECUADOR CELEC EP

Hoja de Ruta

Fecha y hora generación: 2015-01-23 12:39:34 (GMT-5)

Generado por: Diego Fernando Guerrero Bautista

Información del Documento			
No. Documento:	CELEC-EP-2015-0115-MEM	**Doc. Referencia:**	--
De:	Diego Fernando Guerrero Bautista, Subdirector de Tecnología de la Información (E), Corporación Eléctrica del Ecuador	**Para:**	Eduardo Barredo Heinert, Gerente General CELEC EP, Corporación Eléctrica del Ecuador
Asunto:	Solicitud de aprobación y difusión de Normas Técnicas de Seguridad de Información y Guías	**Descripción Anexos:**	--
Fecha Documento:	2015-01-21 (GMT-5)	**Fecha Registro:**	2015-01-21 (GMT-5)

Ruta del documento

Área	De	Fecha/Hora	Acción	Para	No. Días	Comentario
Corporación Eléctrica del Ecuador	María Isabel Carrillo Alvarado (CELEC-EP)	2015-01-22 16:12:03 (GMT-5)	Archivar		1	DOCUMENTO APROBADO, SE ENVÍO MEMORANDO A GERENTES DE UNIDAD Y DIRECTORES CON LINEAMIENTOS Y NORMAS: MEMORANDO NRO. CELEC-EP-2015-0128-MEM
Corporación Eléctrica del Ecuador	María Isabel Carrillo Alvarado (CELEC-EP)	2015-01-22 16:11:54 (GMT-5)	Informar	Diego Fernando Guerrero Bautista (CELEC-EP)	1	DOCUMENTO APROBADO, SE ENVÍO MEMORANDO A GERENTES DE UNIDAD Y DIRECTORES CON LINEAMIENTOS Y NORMAS: MEMORANDO NRO. CELEC-EP-2015-0128-MEM
Corporación Eléctrica del Ecuador	María Isabel Carrillo Alvarado (CELEC-EP)	2015-01-22 16:11:54 (GMT-5)	Informar	Leslye Tatiana Davila Avila (CELEC-EP)	1	DOCUMENTO APROBADO, SE ENVÍO MEMORANDO A GERENTES DE UNIDAD Y DIRECTORES CON LINEAMIENTOS Y NORMAS: MEMORANDO NRO. CELEC-EP-2015-0128-MEM
Corporación Eléctrica del Ecuador	Eduardo Barredo Heinert (CELEC-EP)	2015-01-22 16:11:22 (GMT-5)	Reasignar	María Isabel Carrillo Alvarado (CELEC-EP)	1	Documento tomado por María Isabel Carrillo Alvarado de la Bandeja de Documentos Recibidos de Eduardo Barredo Heinert. DOCUMENTO APROBADO, SE ENVÍO MEMORANDO A GERENTES DE UNIDAD Y DIRECTORES CON LINEAMIENTOS Y NORMAS: MEMORANDO NRO. CELEC-EP-2015-0128-MEM
MAT DGE Tecnologías de la Información	Diego Fernando Guerrero Bautista (CELEC-EP)	2015-01-21 07:51:50 (GMT-5)	Envío Electrónico del Documento		0	
MAT DGE Tecnologías de la Información	Diego Fernando Guerrero Bautista (CELEC-EP)	2015-01-21 07:51:50 (GMT-5)	Firma Digital de Documento		0	Documento Firmado Electrónicamente
MAT DGE Tecnologías de la Información	Diego Fernando Guerrero Bautista (CELEC-EP)	2015-01-21 07:51:02 (GMT-5)	Registro	Eduardo Barredo Heinert (CELEC-EP)	0	Por favor su revisión, aprobación y difusión.

ÍNDICE

Sección I

Norma Técnica de Seguridad de Información

SIC-NTE-001-2014

Revisión 1

Diciembre - 2014

CONTENIDO

INTRODUCCIÓN

La Empresa Pública Estratégica Corporación Eléctrica del Ecuador CELEC EP[1], es la encargada de brindar el servicio de generación y transmisión de energía eléctrica, a nivel nacional, con calidad, economía y seguridad.

En este contexto, es necesario implementar seguridad en sus Activos de Información, tomando como marco de referencia la familia de normas ISO27000, NTE INEN-ISO/IEC 27000 y los estándares internacionales NERC-CIP.

El presente documento está orientado a la búsqueda del cumplimiento de las normas y estándares indicados en el párrafo anterior, lo que podría permitir la certificación futura de toda la Corporación en la normas ISO 27000.

Estas Normas Técnicas comprenden un camino para mejorar el grado de madurez de la Corporación sobre la Seguridad de Información, por lo que su cumplimiento estará supeditado a una programación en base a prioridades y recursos destinados para su aplicación, conforme a lo señalado en el Instructivo de aplicación que se adjunta a este documento.

Periódicamente se revisarán los avances dentro de la Corporación hasta llegar al cumplimiento total.

La presente Norma Técnica está sujeta a revisiones y podrá sufrir modificaciones, de acuerdo a las novedades que se registren en los temas de seguridad de información tratados, los mismos que serán aprobados y debidamente comunicados.

Esta norma técnica será instrumentada mediante Guías Técnicas de Seguridad de Información, las mismas que serán emitidas por el Oficial de Seguridad de CELEC EP.

Se establecerán mecanismos que permitan la socialización y actualización, de esta Norma Técnica, de las Guías de Seguridad y de la documentación asociada.

ALCANCE

La presente Norma Técnica de Seguridad de la Información se crea en cumplimiento de las disposiciones legales, normas, estándares y buenas

[1] En el presente documento se hará referencia a la Empresa Pública Estratégica Corporación Eléctrica del Ecuador CELEC EP, de manera indistinta ya sea como “la Corporación”, “CELEC EP” o “CELEC”.

prácticas nacionales e internacionales vigentes con el objeto de gestionar adecuadamente la seguridad de información en los sistemas informáticos, en el ambiente tecnológico y de comunicaciones de la Corporación y los procesos que reciben y producen información; es decir, en todos los activos de información de CELEC EP.

Esta Norma se aplicará a nivel Corporativo por lo que deberá ser conocida y cumplida por todos los Servidores, conforme se vaya implementando, sea cual fuere su nivel jerárquico y su tipo de dependencia laboral, así como también por terceros que requieran acceso o uso a los activos de información de la Corporación.

OBJETIVO

Normar la protección de los activos de información de la Corporación, tomando en cuenta amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar su disponibilidad, integridad y confidencialidad.

1 LINEAMIENTOS GENERALES

1.1 Asignación de responsabilidades para la seguridad de la información

Los **usuarios de los activos de información** son responsables de conocer y cumplir las Normas y Guías de Seguridad de Información vigentes.

1.1.1 Jefaturas

Todos los Directores, Gerentes o equivalentes, jefes y responsables de las diferentes áreas Organizacionales, a todo nivel jerárquico, son responsables de la implementación de esta Norma Técnica de Seguridad de Información dentro de sus ámbitos de gestión.

1.1.2 Oficial de Seguridad de la Información

De acuerdo a la Resolución de Gerencia General No. CELEC EP-GGE-0026-14, la estrategia de Seguridad de Información de la Corporación y lo estipulado en el Acuerdo Ministerial No. 166, el **Oficial de Seguridad de la Información** tendrá las siguientes responsabilidades:

a) Coordinar los proyectos, así como las actividades de alto nivel, presentes y futuros de las Unidades de Negocio y de Matriz

relacionados con Seguridad de Información en la Corporación, conforme a las necesidades de la misma, al plan estratégico y a las prioridades que puedan ser dictaminadas por la Gerencia General o el Directorio.

b) Conformar y coordinar el Equipo de Seguridad de Información de la Corporación.

c) Proponer y gestionar la aprobación de la normativa y compromisos de confidencialidad relacionados con la seguridad de información.

d) Definir y aprobar las guías, instructivos, procesos y metodologías que soportan a esta Norma Técnica.

e) Conocer y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de información.

f) Aprobar y recomendar las iniciativas que permitan mejorar la seguridad de información, de acuerdo a las competencias y responsabilidades asignadas a cada área[2].

g) Promover la difusión y apoyo a la seguridad de la información dentro de la Corporación.

h) Gestionar la provisión oportuna de recursos económicos, tecnológicos y humanos para la seguridad de la información.

i) Velar por la aplicación de la familia de normas técnicas ecuatorianas NTE INEN-ISO/IEC 27000 y los estándares NERC-CIP o ERNCIP en la Corporación según su ámbito de acción.

j) Velar por la creación del estándar de Ciberseguridad de activos críticos de infraestructura.

k) Aprobar las definiciones propuestas por el Equipo de Seguridad de Información de la Corporación.

l) Autorizar el bloqueo, suspensión, revisión o análisis de los servicios de TIC cuando se considere que existe una amenaza.

m) Mantener contacto apropiado con organizaciones públicas y privadas, asociaciones profesionales y grupos de interés especializados en seguridad de la información para mejorar el conocimiento sobre metodologías y mejores prácticas, que permitan una actualización continua de información pertinente a gestión de la seguridad.

n) Enviar al Subdirector de Tecnologías de la Información y Comunicaciones los informes recibidos de las áreas de TIC y del

[2] Se refiere a dar curso a las propuestas presentadas por parte de las áreas de acuerdo a sus competencias, elevándolas a la máxima autoridad, a través del Equipo de Seguridad de Información, con relación a la seguridad de información de la Corporación.

equipo de Seguridad, siempre y cuando la clasificación de dicho informe se lo permita.

o) Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la Corporación frente a incidentes de seguridad imprevistos y eventos programados (ej. simulacros).

p) Dar seguimiento a los cambios que pueden comprometer a los activos de información, frente a riesgos o amenazas, que pueden afectarlos.

q) Evaluar y coordinar la implementación de controles específicos de seguridad de la información para sistemas o servicios.

r) Verificar el cumplimiento de las lo establecido en los literales c) y d) anteriores, así como de los controles de seguridad implementados en la Corporación.

s) Controlar la existencia de una designación formal como Propietarios de los activos, a los custodios o responsables de la información de las diferentes áreas de la Corporación, conforme al levantamiento de activos de información.

t) Coordinar la gestión de eventos de seguridad con otras entidades nacionales e internacionales.

u) Otras que, por naturaleza de las actividades de gestión de la seguridad de la información, deban ser realizadas.

A partir de la expedición de esta Norma, el Oficial de Seguridad de Información será un miembro activo del Comité de Tecnologías de Información de la Corporación y verificará que, en las actas de reunión, se registren los temas de Seguridad de Información tratados.

1.1.3 Equipo de Seguridad

Además de brindar soporte al Oficial de Seguridad para el cumplimiento de sus funciones, los **Especialistas** que conforman el **Equipo de Seguridad Información de la Corporación** tendrán las siguientes responsabilidades:

a) Elaborar lineamientos de seguridad para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas de seguridad antes de su puesta en servicio.

b) Desarrollar procedimientos para el control de cambios a los procesos operativos, los sistemas e instalaciones, y verificar su cumplimiento, de manera que no afecten de forma negativa la seguridad de la información.

c) Desarrollar procedimientos para el manejo de incidentes derivados del infringimiento de la normativa de seguridad.

d) Desarrollar procedimientos para la administración de medios informáticos de almacenamiento (ej., cintas, discos, etc.) e informes impresos, y verificar la eliminación o destrucción segura de los mismos, cuando proceda.

e) Desarrollar procedimientos adecuados de concienciación de usuarios en materia de seguridad, controles de acceso a los sistemas y administración de cambios.

f) Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso, que garanticen la seguridad de los datos y los servicios conectados a las redes de la Corporación.

g) Verificar la existencia de documentación física o electrónica actualizada relacionada con los procedimientos de comunicaciones, operaciones y sistemas.

h) Verificar que los mecanismos de distribución y difusión de información dentro y fuera de la Corporación incorporen requerimientos de seguridad de información.

i) Dar seguimiento a la socialización e implementación y seguimiento al Compromisos de confidencialidad y de no-divulgación de información, acorde con las leyes y las necesidades de protección de los activos de información.

j) Controlar que los Compromisos de Confidencialidad, documento físico o electrónico, sean firmados de manera física o electrónica por todo el personal de la Corporación, sin excepción, e informar al Oficial de Seguridad de Información sobre el cumplimiento.

k) Controlar que el área de TIC realice la obtención y resguardo de los respaldos de información, así como la prueba periódica de su restauración.

l) Asegurar el registro de las actividades realizadas por el personal operativo de seguridad de la información, para su posterior revisión.

m) Gestionar los incidentes de seguridad de la información de acuerdo a los procedimientos que se establezca.

n) Gestionar la obtención de reportes, advertencias oportunas de alertas, avisos y parches relacionados con ataques y vulnerabilidades de organizaciones públicas, privadas y académicas reconocidas por su aporte a la gestión de la seguridad de la información.

o) Reportar a los Operadores de Seguridad de manera oportuna las advertencias, alertas, avisos y parches relacionados con ataques y vulnerabilidades.

p) Mantener un inventario detallado de Propietarios de la Información, de acuerdo a lo establecido en a la "Guía de Gestión de Activos de Información", adjunta a esta Norma.

q) Alimentar la base de conocimientos de Seguridad de Información Corporativa.

r) Brindar el apoyo técnico a toda la Corporación para el cumplimiento de los controles establecidos en esta Norma y sus documentos de soporte.

s) Entregar los resultados de las actividades de monitoreo, proyecciones y revisión al Oficial de Seguridad de Información una vez que estén disponibles.

t) Otras que por aplicación de esta norma y las guías deban ser realizadas.

1.1.4 Área de Tecnologías de la Información y Comunicaciones

El **Subdirector de Tecnologías de la Información y Comunicaciones** tendrá las siguientes responsabilidades:

a) En coordinación con el Oficial de Seguridad de Información y el área de TIC, realizará el diseño, implementación y mejoramiento de las guías y procedimientos relacionados con la seguridad de la tecnología de información y comunicación, así como el mejoramiento de esta norma.

b) Verificar el cumplimiento de las responsabilidades asignadas de las Áreas de Tecnologías de la Información y Comunicaciones como producto de la aplicación de esta norma, en coordinación con el Equipo de Seguridad.

c) Coordinar la implementar procesos necesarios para el cumplimiento de la normativa de Seguridad de Información, en coordinación con el Equipo de Seguridad.

d) Verificar la ejecución de tareas o actividades especiales de seguridad de información sobre sistemas o equipos relacionados con el núcleo del negocio de la Corporación (ej. SCADA/EMS/GMS/DMS, RAPs), o equipos de Comunicaciones, en coordinación con el Equipo de Seguridad.

e) Otras que por naturaleza de las actividades de su cargo relacionadas con la seguridad de la información deban ser por él realizadas.

Los **Jefes y Responsables de Tecnologías de la Información y Comunicaciones,** tendrá las siguientes responsabilidades:

f) Implementar los controles de seguridad definidos para evitar software malicioso, accesos no autorizados, etc.

g) Implementar procedimientos para la eliminación o destrucción segura de medios informáticos de almacenamiento (ej., cintas, discos, etc.) e informes impresos, cuando proceda.

h) Implementar planes de contingencia que cuenten con medidas técnicas, humanas y organizacionales que permitan garantizar la continuidad de las operaciones en la Corporación.

i) Evaluar el impacto operativo a nivel de seguridad de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación.

j) Evaluar la administración de los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento

k) Verificar el cumplimiento de procedimientos para comunicar las fallas de seguridad en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.Informar al Oficial de Seguridad de Información sobre los incidentes y la operación de Seguridad

l) Verificar el hardware y software (nuevos) para garantizar su compatibilidad con los componentes de otros sistemas y servicios de la Corporación, previo a su adquisición.

m) Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad que procesan para para brindar un adecuado servicio a los usuarios.

n) Otras que por aplicación de esta norma y las guías deban ser realizadas.

En cada **Área de Tecnologías de la Información y Comunicaciones**[3] debe existir al menos un **Operador de Seguridad de Información**, quien tendrá las siguientes responsabilidades:

o) Interlocutor del área de TIC con el equipo de seguridad.

p) Aplicar de manera oportuna los parches y controles relacionados con ataques y vulnerabilidades.

[3] Ver definición en el Glosario de términos.

q) Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad que procesan para soportar potenciales amenazas a la seguridad de la información y para cubrir los niveles de servicio acordados con los usuarios.

r) Otras que por aplicación de esta norma y las guías deban ser realizadas.

1.1.5 Propietario de la Información

Los **Propietarios de la Información**[4] tendrán las siguientes responsabilidades:

a) Verificar, con el Equipo de Seguridad de Información, la correcta aplicación de los controles de seguridad sobre los Activos de Información.

b) Verificar la clasificación de los activos de información de acuerdo con el grado de sensibilidad, criticidad de acuerdo a la "Guía de Gestión de Activos de Información", adjunta a esta Norma.

c) Otras que por aplicación de esta norma y las guías deban ser realizadas.

1.1.6 Responsable de los activos de Información

Los **Responsable de la Información** [5] tendrán las siguientes responsabilidades:

a) Documentar y mantener actualizada la clasificación efectuada.

b) Realizar o delegar tareas de respaldos o recuperación.

c) Definir y efectuar una verificación periódica de los usuarios que deberán tener permisos de acceso a los activos de información de acuerdo a sus funciones y competencia.

d) Autorizar la difusión de información de acuerdo a la "Guía de Gestión de Activos de Información", adjunta a esta Norma.

e) Otras que por aplicación de esta norma y las guías deban ser realizadas.

---

[4] El concepto "de la información" debe ser entendido desde su acepción técnica, no jurídica ACLARAR

[5] El concepto "de la información" debe ser entendido desde su acepción técnica, no jurídica

1.2 Revisión de la Norma Técnica

El Oficial de Seguridad de Información revisará semestralmente la presente Norma Técnica, a efectos de mantenerla actualizada.

Los cambios de fondo serán enviados al Gerente General para su aprobación. Sin embargo, los cambios de forma en la Norma Técnica y sus documentos asociados serán aprobados por el Oficial de Seguridad.

Los cambios de forma incluyen: creación de nuevas guías que soporten a lo establecido en la Norma, eliminación de numerales o literales de la Norma Técnica debido a su inclusión en una Guía, mejoras de redacción, cambios que deban darse por evolución tecnológica, variación de los costos de los controles, impacto de los incidentes de seguridad de información, experiencia de aplicación de la norma, entre otros.

Se podrá encontrar la versión más actual de las Normas y sus Guías en el Sistema de Gestión Documental Corporativo.

1.3 Compromisos de Confidencialidad

a) Al suscribir un compromiso de confidencialidad, los suscriptores aceptan cumplir los requisitos de la seguridad de información de la Corporación mencionados en el mismo.

b) Debe existir la aceptación, entendimiento y firma de compromisos de confidencialidad y de no divulgación de información por parte de terceros (ej., contratistas, proveedores, pasantes, entre otros) así como del personal que tenga relación de dependencia con la Corporación.

c) El Administrador de Contrato o Convenio será el responsable de la suscripción del Compromiso de Confidencialidad por parte de terceros.

El **Subdirector o Jefe del Departamento de Talento Humano** o quién lo reemplace en sus funciones tendrá las siguientes responsabilidades:

d) Notificar a todo el personal que ingresa, sobre sus obligaciones respecto del cumplimiento de la Norma Técnica de Seguridad de Información y de todas las guías, procedimientos y prácticas que de ella surjan.

e) Velar por la suscripción de los Compromisos de Confidencialidad y las tareas de capacitación continua en materia de seguridad de la información.

El área de Talento Humano deberá:

f) Almacenar los compromisos firmados, en los expedientes, físicos o electrónicos de cada Servidor, la firma de los compromisos de confidencialidad debe ser parte de los procedimientos de incorporación de nuevos Servidores a la Corporación, sin excepción.

Para la Gestión de Contratos y Compromiso de Confidencialidad, con los Servidores y con terceros se deberá seguir lo establecido en la "Guía de Contratos y Compromiso de Confidencialidad" adjunta a esta Norma.

1.4 Relación con las autoridades y con terceros

a) Toda relación o contacto oficial con las autoridades internas o externas, con grupos de interés especiales y en general con partes externas (ver punto 1.6) en asuntos de Seguridad de Información deberá realizarse por el Gerente General y/o el Oficial de Seguridad de Información de la Corporación o quién los reemplace en sus funciones.

b) Todo incidente de seguridad de la información que sea considerado crítico deberá ser reportado al Oficial de Seguridad de la Información y éste a su vez a la máxima autoridad según el caso.

c) El Oficial de Seguridad de Información, debe procurar el contacto entre oficiales y responsables de la seguridad de la información para compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades.

d) El administrador de contratos con proveedores o terceros, deben identificar y mantener actualizados los datos de contacto de los proveedores de bienes o servicios de telecomunicaciones o de acceso a la Internet para gestionar potenciales incidentes.

1.5 Revisión independiente de la seguridad de la información

a) El Gerente General podrá solicitar revisiones independientes sobre las actuaciones del Equipo de Seguridad de Información.

El Oficial de Seguridad de Información será el responsable de:

b) Ejecutar revisiones independientes de la gestión de la seguridad a intervalos planificados o cuando ocurran eventos significativos. La revisión podrá contemplar las actuaciones de la alta dirección, y del

oficial de seguridad en materia de gestión de la seguridad.

c) Identificar oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad, incluyendo la normativa y los objetivos de control, a partir de las revisiones independientes.
d) Registrar y documentar todas las revisiones independientes de la gestión de la seguridad de la información que la Corporación realice.

1.6 Consideraciones de seguridad con terceros

Identificación de los riesgos relacionados con las partes externas:

a) El Oficial de Seguridad de Información y su Equipo, en conjunto con el Propietario de la Información, deberá identificar y evaluar los riesgos para la información y los servicios de procesamiento de información de la entidad en los procesos que involucran terceras partes e implementar los controles apropiados antes de autorizar el acceso.

   La evaluación de Riesgos se deberá realizar de acuerdo a lo establecido en la "Guía de Gestión de Riesgos" adjunta a esta Norma.

Relación con ciudadanos o clientes:

b) El Oficial de Seguridad de Información y su Equipo, en conjunto con el Propietario de la Información, deberá identificar requisitos de seguridad antes de facilitar servicios a ciudadanos o clientes de entidades gubernamentales que utilicen o procesen información de los mismos o de la Corporación. Se podrá utilizar uno o varios de los siguientes elementos, según convenga:
   - protección de activos de información;
   - descripción del producto o servicio que va a estar disponible;
   - razones, requisitos y beneficios del acceso del cliente;
   - guía de control del acceso;
   - convenios para gestión de inexactitudes de la información, incidentes de la seguridad de la información y violaciones de la seguridad;
   - nivel de servicio comprometido y los niveles inaceptables de servicio;
   - el derecho a monitorear y revocar cualquier actividad relacionada con los activos de la organización;
   - las respectivas responsabilidades civiles de la organización y del cliente;
   - las responsabilidades relacionadas con asuntos legales y la forma en que se garantice el cumplimiento de los requisitos legales;

- derechos de propiedad intelectual y asignación de derechos de copia y la protección de cualquier trabajo colaborativo;
- protección de datos en base a leyes nacionales, particularmente datos personales o financieros de los ciudadanos.

El **Director, Asesor o Subgerente Jurídico** o quién lo reemplace en sus funciones tendrá las siguiente responsabilidad:

c) Coordinar el cumplimiento de la presente Norma, en lo que corresponde a la gestión de los contratos, acuerdos, compromisos de la Corporación con los Servidores y con terceros, en lo que concierne a aspectos legales.

2 GESTION DE LOS ACTIVOS DE INFORMACIÓN

2.1 Inventario de activos

El inventario de los activos de información, en formatos físicos y/o electrónicos contemplará lo establecido en la "Guía de Gestión de Activos de Información" adjunta a esta Norma Técnica.

2.2 Responsable de los activos

a) El equipo de Seguridad de Información, identificará los activos de información de mayor relevancia en conjunto con el Propietario de la información de las diferentes áreas de CELEC EP, determinando el responsable, su ubicación, niveles de seguridad, para luego elaborar un inventario con dicha información.

b) El Responsable de los activos de Información asociados (o grupos de activos), es el encargado de proteger y mantener la confidencialidad, integridad y disponibilidad de los activos de información.

El detalle sobre las responsabilidades, se encuentra establecido en la "Guía de Gestión de Activos de Información" adjunta a esta Norma Técnica.

2.3 Uso aceptable de los activos

Todos los Servidores, contratistas y usuarios por terceras parte deben seguir las reglas para el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de información.

El detalle sobre el uso aceptable de los activos de información se encuentra en la “Guía de Gestión de Activos de Información”, anexo a ésta Norma.

2.4 Directrices de clasificación de la información

La información se deberá clasificar en términos de valor, de los requisitos legales, de la sensibilidad y la importancia hacia la Corporación.

La metodología de clasificación de activos se encuentra detallada en el documento “Guía de Gestión de Activos de Información”, anexo a ésta Norma.

2.5 Etiquetado y manejo de la información

El etiquetado y manejo de información en formato físico o digital, debe estar de acuerdo al esquema de clasificación adoptado por la Corporación (ver punto 2.4), mediante abreviaturas, acerca del tipo de activo y su funcionalidad para la generación de etiquetas.

El detalle sobre el etiquetado y manejo de la información se encuentra en la “Guía de Gestión de Activos de Información” anexo a ésta Norma Técnica.

3 SEGURIDAD DE INFORMACIÓN RELACIONADA CON EL PERSONAL

3.1 Funciones y responsabilidades

a) El área de Talento Humano deberá permitir al Equipo de Seguridad de Información, el acceso al listado de Servidores en nómina con información actualizada (cargo, datos personales, identificación personal, correo electrónico) para verificar de manera periódica, el listado de usuarios en los sistemas administrados por TIC con el listado entregado por Talento Humano. De existir errores, el Oficial de Seguridad de Información solicitará al área de TIC su corrección.

3.2 Selección

El área de Talento Humano deberá:

a) Verificar que los antecedentes de candidatos a ser Servidores,

contratistas o usuarios de terceras partes, o designaciones y promociones de Servidores estén de conformidad con la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos. No debe entenderse este control como discriminatorio en ningún aspecto.

b) Definir los criterios y las limitaciones para las revisiones indicadas en el literal anterior.

c) Informar del procedimiento de revisión (por motivos de designación o promoción), y solicitar el consentimiento al personal actual, potenciales Servidores y de terceras partes.

3.3 Términos y condiciones laborales

El área de Talento Humano deberá:

a) Solicitar la firma de un compromiso de confidencialidad, antes de que los Servidores tengan acceso a la información.

b) Establecer mecanismos para socializar los derechos y responsabilidades de los Servidores, los contratistas y cualquier otro usuario sobre la protección de información; incluyendo constancia de lo actuado a través de hojas de registro, informes o similares, que evidencie la realización de la misma.

3.4 Educación, formación y sensibilización en seguridad de la información

a) El Oficial de Seguridad de Información deberá coordinar la emisión de boletines informativos de alertas de seguridad con información precisa mediante Comunicación Corporativa.

b) El Oficial de Seguridad de Información recomendará a los responsables de área de la Corporación la asistencia de sus especialistas a cursos de seguridad relativos a su ámbito de acción.

c) El Equipo de Seguridad de información deberá socializar y capacitar de forma oportuna y periódica, en lo relativo a la seguridad de información, sobre las normas y los procedimientos, las responsabilidades legales y los controles de la Corporación, así como en la capacitación en seguridad para el uso correcto de los servicios de información a todos los Servidores de la Corporación.

El detalle sobre la sensibilización y el cambio de cultura organizacional de seguridad de la información se encuentra en la "Guía de Sensibilización de la Seguridad de Información Corporativa al usuario", anexo a ésta Norma Técnica.

3.5 Devolución de activos y retiro de privilegios de acceso

El área de Talento Humano deberá:

a) Formalizar el procedimiento de terminación del contrato laboral, en el cual se incluya la devolución de software, documentos corporativos, equipos, y otros activos de la Corporación tales como los dispositivos de cómputo móviles, tarjetas de crédito, las tarjetas de acceso, tokens USB con certificados de electrónicos, certificados electrónicos en archivo, memorias flash, teléfonos celulares, cámaras, manuales, información almacenada en medios electrónicos y otros entregados.

b) Notificar al Oficial de Seguridad la finalización o cambio en la relación que el Servidor, contratista o tercero tiene con la Corporación, para proceder con cambio o retiro de los derechos de acceso a los activo de información y a los servicios e procesamiento de información.

c) El Oficial de Seguridad de Información coordinará la verificación del retiro de los derechos de acceso a la información y a los servicios de procesamiento de información (ej., sistema de directorio, correo electrónico, accesos físicos, aplicaciones de software, etc.), por parte del área de TIC.

El detalle sobre la devolución de activos de información y retiro de privilegios de acceso se encuentra en la "Guía de Gestión de Activos de Información" adjunta a esta Norma Técnica, anexo a ésta Norma Técnica

4 SEGURIDAD FISICA Y DEL ENTORNO

Estos puntos de la Norma deberán ser cubiertos por varias áreas, en especial Servicios Generales, TIC y el Equipo de Seguridad. Para la implementación de controles, el Oficial de Seguridad de Información designará un coordinador, quien a su vez recibirá el apoyo de todas las áreas competentes.

Se aclara que el alcance de todos los puntos de este título está enmarcado en la gestión adecuada de la seguridad de información en los sistemas informáticos, en el ambiente tecnológico y de comunicaciones de la Corporación y los procesos que reciben y producen información; es decir, en todos los activos de información de CELEC EP.

Se definen los siguientes sitios como áreas críticas protegidas:

- Centros de Control de Generación, Transmisión y Distribución.
- Centros de Datos (Salas de Servidores).
- Sistemas de protección, supervisión, control y medición en generación y subestaciones.
- Bóvedas de Seguridad.

4.1 Perímetro de la seguridad física

a) Los Operadores de Seguridad de Información, en coordinación con los responsables de Seguridad Industrial, deberán documentar y definir (respectivamente) claramente los perímetros de seguridad (barreras, paredes, puertas de acceso controladas con tarjeta, etc.).

b) Los Operadores de Seguridad enviarán al Oficial de Seguridad de Información un reporte con Información actualizada de los sitios protegidos, indicando:
   - Identificación del Área.
   - Principales elementos a proteger.
   - Medidas de protección física.

El área de TIC deberá:

c) Aislar los ambientes de procesamiento de información propios de los ambientes proporcionados por terceros.

Los responsables de Servicios Generales serán:

d) Los encargados de vigilar que se definan medios para controlar el acceso físico al lugar o edificio.

e) Los encargados, con apoyo del área de TIC, de coordinar la instalación y buen funcionamiento de un sistema de vigilancia preferentemente mediante el uso de circuitos cerrados de televisión en las áreas restringidas que se determine.

Los responsables de Seguridad Industrial deberán:

f) Coordinar la instalación de alarmas de incendio y puertas de evacuación debidamente monitoreadas que cumplan normas establecidas.

g) Coordinar la protección de las instalaciones críticas de tal manera que

se evite el acceso al personal no autorizado.

4.2 Controles de acceso físico

a) Todos los Responsables de la información deben controlar y limitar el acceso no autorizado, evitando el daño a los activos de información de la Corporación.

b) Los Responsables a cargo de áreas críticas protegidas, deberán revisar, actualizar y documentar cada 4 meses los derechos de accesos a dichas áreas.

El área de Servicios Generales será la encargada de:

c) Implementar medidas para supervisar la permanencia de los visitantes en las áreas restringidas y registrar la hora y fecha de su ingreso y salida (físico y digital cuando sea posible).

d) Coordinar con el área de Talento Humano, el uso de una identificación visible para todo el personal y visitantes, quienes deberán ser escoltados por una persona autorizada para el tránsito en las áreas restringidas.

4.3 Seguridad de oficinas, recintos e instalaciones.

Todos los Servidores deberán:

a) Vigilar que las puertas y ventanas permanezcan cerradas, especialmente cuando no haya vigilancia.

b) Aplicar los reglamentos y las normas en materia de sanidad y seguridad.

Las áreas de TIC deberán:

c) Garantizar que existan sitios alternos de procesamiento de datos, para proceso críticos.

d) Implementar mecanismos de control para la detección de intrusos.

e) Ubicar las impresoras, copiadoras, etc., en un área vigilada.

El área de Seguridad Industrial deberá:

f) Establecer que los sitios de procesamiento sean discretos y tengan un señalamiento mínimo apropiado.

g) Suministrar y dar mantenimiento al equipo contra incendios y ubicarlo adecuadamente.

h) Adoptar controles para minimizar el riesgo de amenazas físicas potenciales como robo, incendio, explosión, humo, agua, polvo, vibración, efectos químicos, plagas, interferencia del suministro eléctrico e interferencia a las comunicaciones.

Los Responsables a cargo de áreas críticas protegidas, deberán realizar las gestiones necesarias para:

i) Que las instalaciones de áreas críticas estén protegidas de tal manera que se evite el acceso no autorizado al público.

j) Con el apoyo del área de Seguridad Industrial, que el almacenamiento de los materiales o combustibles peligrosos, esté a una distancia prudente de las áreas protegidas.

k) En conjunto con las áreas de TIC y Servicios Generales, que el mantenimiento de las instalaciones eléctricas y UPS, de los sistemas de climatización y ductos de ventilación, estén de acuerdo a la recomendación del fabricante .

En los casos que sea necesario, el Operador de Seguridad de Información interactuará con el área de respectiva para implementar las protecciones sobre los activos informáticos y áreas protegidas.

4.4 Trabajo en áreas seguras

Los Responsables a cargo de áreas críticas protegidas con apoyo del Operador de Seguridad de Información deberán:

a) Dar a conocer al personal, la existencia de un área segura y las actividades que pueden realizarse dentro de ella en función de la necesidad.

b) Evitar el trabajo no supervisado en áreas seguras, por razones de seguridad como por ejemplo para evitar la oportunidad de actividades maliciosas.

c) Evitar ingreso de equipos de grabación, cámaras, equipos de vídeo y audio, dispositivos móviles, etc., a menos de que estén autorizados.

d) Revisar periódicamente y disponer de un bloqueo físico de las áreas seguras vacías.

4.5 Áreas de carga, despacho y acceso público

Los Responsables a cargo de áreas críticas protegidas en coordinación con Seguridad Industrial deberán:

a) Controlar los puntos de acceso como área de despacho y carga, por donde podría ingresar personal hacia las áreas protegidas. De ser posible, aislarlos de los servicios de procesamiento de información para evitar accesos no autorizados.

b) Permitir el acceso al área de despacho y carga de equipos informáticos, únicamente a personal identificado y autorizado.

4.6 Ubicación y protección de los equipos

Los Responsables a cargo de áreas críticas protegidas en coordinación con Seguridad Industrial deberán:

a) Ubicar los equipos de modo que se elimine el acceso innecesario a las áreas de trabajo restringidas.

b) Aislar, a medida de lo posible, los servicios de procesamiento de información con datos sensibles y elementos que requieran protección especial, para reducir el riesgo de visualización de la información de personas no autorizadas.

c) Disponer de métodos especiales de protección para equipos informáticos en ambientes industriales, y el monitoreo de las condiciones ambientales de temperatura y humedad.

4.7 Servicios de suministro eléctrico

Los Responsables a cargo de áreas críticas protegidas en coordinación con Seguridad Industrial deberán:

a) Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía para activos de información críticos, cuando sea posible.

b) Implementar y documentar los servicios de electricidad, agua,

calefacción, ventilación y aire acondicionado, suministrados a la Corporación.

c) Inspeccionar regularmente todos los sistemas de suministro.

d) Tener un sistema de suministro de energía sin interrupción (UPS) o al menos permitir el cierre/apagado ordenado de los servicios y equipos que soportan las operaciones críticas de los servicios informáticos de la Corporación.

e) Disponer para las áreas protegidas, de los interruptores cerca de las salidas, para suspender el paso de energía eléctrica, en caso de un incidente o problema.

4.8 Seguridad del Cableado Estructurado

Los Operadores de Seguridad de Información, en coordinación con los responsables a cargo de áreas críticas protegidas deberán:

a) Cumplir con los requisitos técnicos y legales vigentes de la República del Ecuador y Normas Internacionales (ISO, IEEE y NERC, según aplique).

b) Proteger el cableado de la red contra la interceptación o daño, el mismo que debe ser identificado y rotulado de acuerdo a normas locales o internacionales para evitar errores en el manejo.

c) Disponer de documentación, diseños/planos y la distribución de conexiones de redes alámbricas/inalámbricas (locales y remotas), voz, eléctricas, etc.

El área de TIC, en coordinación con los responsables a cargo de áreas críticas protegidas deberá:

d) Controlar el acceso a los módulos de cableado de conexión (patch panel) y cuartos de cableado.

e) Disponer de líneas de fuerza (energía) y de telecomunicaciones protegidas. En cuanto sea posible, los cables de energía de los cables de comunicaciones deben estar separados. En lo posible las instalaciones deben ser subterráneas.

Para los sistemas sensibles o críticos, como la red de comunicaciones por fibra óptica, se implementarán los siguientes controles adicionales, en donde sea necesario:

f) Instalar conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección.

g) A la medida de lo posible, utilizar rutas o medios de transmisión alternativos, en las redes troncales.

4.9 Mantenimiento de los equipos

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Incluir en los procesos de contratación que tengan que ver con equipos por lo menos lo estipulado para el mantenimiento y garantías de equipos dispuestos por el SERCOP.

b) Brindar mantenimientos periódicos a los equipos y dispositivos, de acuerdo a las especificaciones y recomendaciones del fabricante, el mismo que lo debe realizar con personal calificado y autorizado.

c) Conservar los registros de los mantenimientos preventivos, correctivos y fallas relevantes o sospechosas.

d) Establecer controles apropiados para realizar mantenimientos programados y emergentes.

e) Gestionar mantenimientos planificados con hora de inicio, fin, impacto y responsables y poner previamente en conocimiento de administradores y usuarios finales.

f) Registrar el retiro de equipamiento de la sede de la corporación para su mantenimiento, de ser el caso.

g) Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

En el caso de equipos de computación especiales, que no están a cargo del área de TIC (como los del Centro de Control y sistemas de telecomunicaciones), o equipos informáticos como los que están en a las centrales y subestaciones, se los someterá a tareas de mantenimiento preventivo con el conocimiento de los responsables de cada Proyecto o Unidad Organizacional afectada.

4.10 Seguridad de los equipos fuera de las instalaciones

a) Los Responsables de los activos de información deberán custodiar los equipos y medios de información que se encuentren fuera de las instalaciones de la Corporación, tomando en cuenta las instrucciones para la protección de los equipos que se encuentran fuera de estas instalaciones.

b) El Operador de Seguridad de Información, en coordinación con el responsable del área de TIC, deberá disponer de controles para el trabajo que se realiza en equipos informáticos fuera de las instalaciones, mediante una evaluación de riesgos.

c) El área de Seguros, en coordinación con el responsable del área de TIC y del área de Servicios Generales, deberá gestionar una cobertura adecuada del seguro, para proteger los equipos que se encuentran fuera de las instalaciones.

5 GESTION DE COMUNICACIONES Y OPERACIONES DE SEGURIDAD

El alcance de todos los puntos de este título está enmarcado en la gestión adecuada de la seguridad de información en los sistemas informáticos, en el ambiente tecnológico y de comunicaciones de la Corporación y los procesos que reciben y producen información; es decir, en todos los activos de información de CELEC EP.

5.1 Documentación de los procedimientos de operación

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Documentar los procesos de los servicios de procesamiento de datos, incluyendo la interrelación con otros sistemas, y el proceso de respaldo y restauración de la información.

El Operador de Seguridad de Información en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

b) Documentar las instrucciones para el manejo de errores y otras condiciones excepcionales que pueden surgir durante la ejecución de las tareas.

c) Documentar los contactos de soporte, necesarios en caso de incidentes. Esta documentación deberá ser entregada también al Oficial de Seguridad de Información y deberá ser actualizada periódicamente (por lo menos 1 vez cada 6 meses).

d) Documentar las instrucciones para el manejo de medios e informes especiales, incluyendo procedimientos para la eliminación segura de informes fallidos.

e) Documentar los procedimientos para reinicio y recuperación de los sistemas en caso de fallas.

f) Documentar los registros de auditoría y de la información de registro de los sistemas.

5.2 Gestión de Cambios

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control en conjunto con el Equipo de Seguridad deberá establecer responsables y procedimientos formales del control de cambios en los equipos y software. Los cambios deben efectuarse cuando haya razón válida para el negocio, como: cambio de versión, corrección de vulnerabilidades, costos, licenciamiento, nuevo hardware, entre otros.

El detalle sobre este tema se encuentra en la “Guía de Gestión de Cambios” adjunta a esta Norma Técnica, anexo a ésta Norma Técnica

5.3 Distribución y separación de funciones

El Responsable de área, en conjunto con el Propietario del activo de información deberá:

a) Distribuir las funciones y las áreas de responsabilidad, para reducir oportunidades de modificaciones no autorizadas, no intencionales, o el uso inadecuado de los activos de información de la Corporación.

b) Limitar el acceso a modificar o utilizar los activos sensibles sin su respectiva autorización.

El Operador de Seguridad de Información, en conjunto con el Propietario de los activos de información deberá:

c) Establecer controles que evidencie el monitoreo de actividades, registros de auditoría y supervisión por parte del responsable del área.

d) Definir procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana.

5.4 Separación de las instancias de Capacitación, Implementación y Producción

El jefe o responsable del área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Identificar los grados de separación, de los ambientes de capacitación, implementación y producción, para prevenir futuros problemas operativos, e implementar los controles adecuados.

b) Implantar ambientes de prueba, aislados de los ambientes de capacitación y producción, evitando el acceso no autorizado de los datos sensibles. Utilizar sistemas de autenticación y autorización independientes para las diversas instancias o ambientes.

El Operador de Seguridad de Información en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

c) Definir y documentar diferentes entornos para capacitación, implementación, y producción. Para el caso que no se pueda definir diferentes entornos con recursos físicos independientes, se debe mantener diferentes directorios con su respectiva versión y delegación de acceso.

d) Controlar la instalación y uso de herramientas de desarrollo de software y/o acceso a bases de datos y redes en los equipos, salvo que sean parte de las herramientas de uso estándar o su instalación sea autorizada de acuerdo a un procedimiento expresamente definido.

e) Permitir, al personal de implementación de software, el acceso al entorno de producción, únicamente en caso de extrema necesidad, con la autorización explícita correspondiente.

f) Definir perfiles de usuario para las diferentes instancias o ambientes.

5.5 Prestación del Servicio por terceros

El Equipo de Seguridad de Información se encargará de:

a) Establecer controles sobre definiciones del servicio y niveles de

prestación del servicio, para que sean aplicados por terceros.

b) Establecer controles de cumplimiento de terceros, que garanticen la capacidad de servicio, planes ejecutables y diseños para la continuidad del negocio, en caso de desastres.

5.6 Monitoreo y revisión de los servicios por terceros

El Subdirector de TIC, en conjunto con los Jefes del área de TIC deberá:

a) Identificar los sistemas sensibles o críticos que convenga tener dentro o fuera de la Corporación e informar al Comité de Tecnología de Información.

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberán:

b) Monitorear los niveles de desempeño de los servicios para verificar el cumplimiento de los convenios.

c) Analizar los reportes de servicios, reportes de incidentes elaborados por terceros y acordar reuniones periódicas según los acuerdos.

El Operador de Seguridad de Información en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

d) Revisar y verificar los registros y pruebas de auditoría de terceros, con respecto a eventos de seguridad, problemas de operación, fallas relacionados con el servicio prestado.

e) El monitoreo y revisión deberá ser periódico (por lo menos una vez cada 3 meses), de acuerdo a lo establecido en cada contrato y/o convenio.

5.7 Gestión de los cambios en los servicios ofrecidos por terceros

El Operador de Seguridad de Información en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Establecer un proceso de gestión de cambios en los servicios ofrecidos por terceros, en el desarrollo de aplicaciones, provisión de servicios de hardware, software, redes entre otros.

b) Coordinar el proceso de cambio cuando se necesita realizar cambios o mejoras a las redes y uso de nuevas tecnologías en los servicios ofrecidos por terceros.

c) Coordinar el proceso de cambio cuando se realice cambio de proveedores, cambio de ubicación física en los servicios ofrecidos por terceros.

5.8 Gestión de la capacidad

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Realizar proyecciones de los requerimientos de capacidad futura de recursos para asegurar el desempeño de los servicios y sistemas.

b) Monitorear los recursos asignados para garantizar la capacidad y rendimiento de los servicios y sistemas.

c) Utilizar la información del monitoreo para la adquisición, asignación de recursos y evitar cuellos de botella.

5.9 Aceptación del Sistema

El Subdirector de TIC en conjunto con el Oficial de Seguridad de Información deberá:

a) Considerar el efecto que tiene el nuevo sistema en la seguridad global de la Corporación.

b) Garantizar la implementación de un conjunto de controles de seguridad acordados.

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

c) Verificar el desempeño y los requerimientos de cómputo necesarios para los nuevos sistemas.

d) Considerar procedimientos de recuperación y planes de contingencia.

e) Poner a prueba procedimientos operativos de rutina según normas definidas para el sistema.

f) Asegurar que la instalación del nuevo sistema no afecte negativamente los sistemas existentes, especialmente en períodos pico de procesamiento.

g) Capacitar sobre el funcionamiento y utilización de un nuevo sistema.

h) Para nuevos desarrollos, se debe involucrar a los usuarios y a todas las áreas relacionadas, en todas las fases del proceso, garantizando así la eficacia operativa del sistema propuesto.

5.10 Controles contra código malicioso

El Equipo de Seguridad de Información se encargará de:

a) Establecer procedimientos para evitar riesgos en la obtención/descarga de archivos y software desde o a través de redes externas o por cualquier otro medio.

b) Implementar procedimientos para verificar toda la información relativa a software malicioso.

El Operador de Seguridad de Información en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

c) Instalar y actualizar periódicamente software de antivirus y contra código malicioso.

d) Mantener los sistemas operativos y sistemas de procesamiento de información actualizados con las últimas parches de seguridad disponibles.

e) Revisar periódicamente el software y datos de los equipos de procesamiento que sustentan procesos críticos de la Corporación.

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

g) Contratar con el proveedor de Internet o del canal de datos los servicios de filtrado de: virus, spam, programas maliciosos (malware), en el perímetro externo, de ser posible.

5.11 Controles contra códigos móviles

El Operador de Seguridad de Información en conjunto con el área de TIC y/o

Administradores de Sistemas de Centros de Operación y Control deberá:

a) Aislar de forma lógica los dispositivos móviles (equipos smart, tablet, ipad) en forma similar a lo que ocurre con las VLANs.

b) Gestionar el código móvil (software de transferencia entre sistemas) mediante procedimientos de auditoría y medidas técnicas disponibles, bloqueando códigos móviles no autorizados.

c) Establecer, en lo posible, controles criptográficos para autenticar de forma única el código móvil.

5.12 Respaldo de la información

El Operador de Seguridad de Información en conjunto con el equipo Seguridad de Información deberá establecer procedimientos para implementar estrategias de respaldo, para realizar copias de seguridad de los datos y probar sus tiempos de restauración.

El detalle sobre respaldos de información se encuentra en la "Guía de Respaldos" adjunta a esta Norma Técnica.

5.13 Gestión de Seguridad de las redes

El Equipo de Seguridad de Información se encargará de:

a) Establecer controles especiales para salvaguardar la confidencialidad y la integridad de los datos que pasan por las redes públicas, redes locales e inalámbricas.

El Operador de Seguridad de la información en conjunto con el área de TIC deberá:

b) Mantener y controlar adecuadamente los equipos de Seguridad Perimetral para proteger de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red.

5.14 Control de redes

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Establecer procedimientos y definir responsabilidades para la gestión

de equipos remotos como el caso de re-direccionamiento de puertos y accesos por VPNs, incluyendo el área de operaciones y el área de usuarios finales.

b) Disponer de un esquema de red de los enlaces de datos, Internet y redes locales, así como la documentación respectiva.

El Operador de Seguridad de Información en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

c) Garantizar la aplicación de los controles mediante actividades de supervisión.

5.15 Seguridad de los servicios de red

El Operador de Seguridad de Información en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control a medida de lo posible, deberá:

a) Incorporar tecnología para la seguridad de los servicios de red como la autenticación, encriptación y controles de conexión de red.

b) Implementar soluciones que proporcionen valor agregado a las conexiones y servicios de red, como la implementación de firewalls, IPS, antivirus, etc.

c) Definir procedimientos para la utilización de los servicios de red para restringir el acceso a los servicios de red cuando sea necesario.

d) Controlar la incorporación de una zona desmilitarizada (DMZ) o red perimetral que aísle la red corporativa de las aplicaciones disponibles para el público. Los servicios públicos que deben ser accesibles desde la red exterior deberán situarse en la DMZ.

5.16 Seguridad de la documentación del sistema

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Guardar con seguridad toda la documentación de los sistemas.

b) Mantener una lista de acceso mínima a la documentación del sistema y con su debida autorización.

c) Mantener una protección adecuada de la documentación del sistema expuesta en la red pública.

5.17 Medios físicos en tránsito

El área de Servicios Generales, para motivos de seguridad de información, deberá:

a) Utilizar transporte seguro o servicios de mensajería.

b) Embalar de forma segura medios o información enviada a través de servicios de mensajería, en lo posible siguiendo las especificaciones del proveedor o del fabricante.

c) Adoptar controles especiales cuando sea necesario proteger información sensible, contra su divulgación y modificación.

El área de TIC deberá:

d) Definir procedimientos para la utilización y manejo de los medios físicos en tránsito, cuando sea necesario.

5.18 Mensajería electrónica

El Oficial de Seguridad de Información deberá:

a) Establecer lineamientos para proteger los mensajes contra los accesos no autorizados, modificación o denegación de los servicios tomando en cuenta consideraciones legales.

El Equipo de Seguridad de Información deberá:

b) Monitorear los mensajes de acuerdo al procedimiento que se establezca en la Corporación.

El Operador de Seguridad de Información en conjunto con el área de TIC deberá:

c) Encriptar los contenidos y/o información sensibles que puedan enviarse por mensajería electrónica, utilizando firmas electrónicas reconocidas por el Estado Ecuatoriano u otras tecnologías evaluadas y aprobadas por la Corporación o el Gobierno Nacional.

5.19 Sistemas de información del negocio

El Oficial de Seguridad de Información deberá:

a) Establecer normas y controles adecuados para gestionar la forma en que se comparte la información.

b) Establecer requisitos y disposiciones para activación de acciones de emergencia.

El Equipo de Seguridad de Información en conjunto con los propietarios de los activos deberá:

c) Categorizar la información sensible y documentos clasificados.

d) Categorizar al personal, contratistas y usuarios que tengan acceso a los sistemas informáticos y los sitios desde cuales pueden acceder.

El Operador de Seguridad de Información en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

e) Proteger o tener en cuenta las vulnerabilidades conocidas en los sistemas administrativos, financieros, y demás sistemas informáticos donde la información es compartida.

f) Proteger y tener en cuenta las vulnerabilidades en los sistemas de comunicación del negocio como la grabación de las llamadas telefónicas.

g) Implementar controles de acceso a la información como acceso a proyectos confidenciales.

h) Identificar el estado (ACTIVO, INACTIVO, BLOQUEADO) de las cuentas de usuario.

El detalle sobre el manejo de activos como su clasificación y controles se encuentra en la “Guía de Gestión de Activos de Información”, adjunta a esta Norma Técnica.

5.20 Transacciones en línea

El Operador de Seguridad de Información en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Definir procedimientos para el uso de certificados electrónicos con otras instituciones y para garantizar todos los aspectos en la transacción como credenciales de usuario, confidencialidad de la transacción y privacidad de las partes.

b) Cifrar o encriptar el canal de comunicaciones entre las partes involucradas (por ejemplo, utilizando SSL/TLS).

c) Establecer protocolos seguros en la comunicación de las partes involucradas por ejemplo, utilizando SSL/TLS).

d) Establecer procedimientos para que las transacciones se encuentren fuera del entorno de acceso público.

e) Utilizar los servicios de una entidad certificadora confiable, cuando sean requeridos.

5.21 Información disponible al público

El Operador de Seguridad de Información en conjunto con el área de TIC deberá:

a) Implementar controles para que la información disponible al público se encuentre conforme a la normativa vigente.

b) Implementar procedimientos para que la información sensible no esté disponible al público y sea protegida durante la recolección, procesamiento y almacenamiento.

El detalle sobre el manejo de activos como su clasificación y controles se encuentra en la "Guía de Gestión de Activos de Información", adjunta a esta Norma Técnica.

5.22 Registros para auditorías y Monitoreo de uso del sistema

El Operador de Seguridad de Información en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Registrar los accesos autorizados y no autorizados, incluyendo:
    - Identificación del ID de usuario;
    - Fecha y hora de eventos clave;
    - Tipos de evento;
    - Archivos a los que se han tenido acceso;

- Programas y utilitarios utilizados;

b) Registrar y monitorear las operaciones privilegiadas, como
   - Uso de cuentas privilegiadas;
   - Encendido y detección del sistema;
   - Acople y desacople de dispositivos de entrada;

c) Registrar y monitorear intentos de acceso no autorizados, como:
   - Acciones de usuario fallidas o rechazadas;
   - Violación de la política de acceso y notificaciones de firewalls y gateways;
   - Alertas de los sistemas de detección y prevención de intrusos;

d) Registrar y revisar alertas o fallas del sistema, como:
   - Alertas y/o mensajes de consola;
   - Excepciones de registro del sistema;
   - Alarmas de gestión de red;
   - Alarmas del sistema de control de acceso;

e) Registrar y revisar cambios o intentos de cambio en la configuración y los controles de la seguridad del sistema.

f) Establecer procedimientos para el monitoreo de uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo.

g) Registrar la fecha, hora y detalles de los eventos clave, como registro de inicio y registro de cierre.

h) Registrar la terminal si es posible.

i) Registrar el uso de las aplicaciones y sistemas.

j) Registrar las direcciones y protocolos de red.

k) Definir alarmas originadas por el sistema de control de acceso.

l) Activación y desactivación de los sistemas de protección como antivirus y los sistemas de detección y prevención de intrusos.

5.23 Sincronización de relojes

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Sincronizar los relojes de los sistemas de procesamiento de información pertinentes con una fuente de tiempo exacta (ejemplo el tiempo coordinado universal o el tiempo estándar local). En lo posible, se deberá sincronizar los relojes en base a un protocolo o servicio de tiempo de red para mantener todos los equipos sincronizados.

b) Verificar y corregir cualquier variación significativa de los relojes sobretodo en sistemas de procesamiento donde el tiempo es un factor clave.

c) Garantizar que la marca de tiempo refleja la fecha/hora real considerando especificaciones locales (por ejemplo, el horario de Galápagos o de países en donde existen.

d) Garantizar la configuración correcta de los relojes para la exactitud de los registros de auditoría o control de transacciones y evitar repudio de las mismas debido a aspectos del tiempo.

El Operador de Seguridad de Información verificará que estas actividades se lleven a cabo.

6 CONTROL DEL ACCESO A LOS SISTEMAS DE INFORMACIÓN

6.1 Controles de acceso

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Gestionar los accesos de los usuarios a los sistemas de información, asegurando el acceso de usuarios autorizados y previniendo los accesos no autorizados.

El detalle sobre el control de acceso se encuentra en la “Guía de Control de Acceso” adjunta a esta Norma Técnica.

6.2 Registro de usuarios

El Operador de Seguridad de Información en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Establecer un procedimiento formal, documentado y difundido, en la administración de los perfiles y roles de las cuentas de los usuarios de acuerdo a lo detallado en la "Guía de control de acceso" adjunta a esta Norma Técnica.

b) Para el caso de usuarios genéricos, se procederá de acuerdo a lo especificado en la "Guía de control de acceso" adjunta a esta Norma Técnica.

6.3 Gestión de privilegios

El Operador de Seguridad de Información en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá controlar la asignación de privilegios, de conformidad con la "Guía de control de acceso".

6.4 Revisión de los derechos de acceso de los usuarios

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Realizar las depuraciones respectivas de los accesos de los usuarios, determinando un periodo máximo de 10 días; en casos de presentar cambios estructurales, esta gestión deberá hacerse inmediatamente que se ejecute el cambio organizacional.

b) Evidenciar los cambios sobre los derechos de acceso en archivos de log o registro de los sistemas, los cuales deben estar disponibles en caso que se requieran.

6.5 Uso de los servicios de red

El área de TIC deberá:

a) Levantar un registro de los servicios de red de la Corporación.

b) Identificar por cada servicio los grupos de usuarios que deben acceder.

c) Definir los perfiles y roles para cada grupo de usuarios que tenga acceso a la red y sus servicios.

d) Definir mecanismos de bloqueos para que sea restringido el acceso de

equipos a la red.

6.6 Separación en las redes

El Equipo de Seguridad de Información deberá:

a) Realizar una evaluación de riesgos para identificar los segmentos de red donde se encuentren los activos críticos para la Corporación.

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control, en la medida de lo posible deberá:

b) Dividir las redes en dominios lógicos de red, dominios de red interna, dominios de red externa e inalámbrica.

c) Documentar la segregación de red, identificando las direcciones IP que se encuentran en cada segmento de red.

d) Configurar la puerta de enlace (gateway) para filtrar el tráfico entre dominios y bloquear el acceso no autorizado.

e) Controlar los flujos de datos de red usando las capacidades de enrutamiento/conmutación (ej., listas de control de acceso).

f) Ejecutar la separación de las redes en base a la clasificación de la información almacenada o procesada en la red, considerando que el objetivo es dar mayor protección a los activos de información críticos en función del riesgo que éstos podrían presentar.

g) Separar redes inalámbricas procedentes de redes internas y privadas, para evitar el acceso a terceros y de usuarios externos a las redes privadas internas.

El Operador de Seguridad de Información verificará que estas actividades se lleven a cabo.

6.7 Control del enrutamiento en la red

El Operador de Seguridad de Información en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Configurar políticas de control de acceso para el enrutamiento en la red, basándose en los requerimientos de la Corporación. Para este caso, el enrutamiento por defecto no será aceptado.

Las puertas de enlace de la seguridad (gateway) se pueden usar para validar la dirección fuente/destino en los puntos de control de las redes internas y externas, si se emplean tecnologías proxy y/o de traducción de direcciones de red.

6.8 Restricción de acceso a los sistemas de información

El Equipo de Seguridad, deberá realizar revisiones periódicas cada 6 meses, para garantizar el retiro de permisos de acceso no autorizados en los sistemas de información.

El Operador de Seguridad de Información en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Controlar el acceso a las funciones de los sistemas y aplicaciones.

b) Definir mecanismos de control para los derechos de acceso de los usuarios, para lectura, escritura, eliminación y ejecución de información.

c) Definir y documentar mecanismos de control para los derechos de acceso entre aplicaciones.

d) Generar mecanismos a fin de garantizar que los datos de salida de los sistemas de aplicación que manejan información sensible sólo contengan la información pertinente y que se envíe únicamente a terminales o sitios autorizados.

6.9 Aislamiento de sistemas sensibles

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá garantizar que:

a) Las aplicaciones sensibles, por su criticidad para la Corporación, se ejecuten en equipos adecuados y robustos, únicamente compartir recursos con sistemas de aplicación confiables, o utilizar métodos físicos o lógicos de aislamiento.

El Operador de Seguridad de Información en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

b) Identificar y registrar los riesgos, cuando una aplicación se ejecuta en un entorno compartido.

c) Identificar y registrar aplicaciones sensibles que se encuentra compartiendo recursos.

6.10 Computación y comunicaciones móviles

El Operador de Seguridad de Información en conjunto con el área de TIC deberá:

a) Establecer un procedimiento para adoptar medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de equipos informáticos.

b) Asistir a los Servidores para respaldar y resguardar la información sensible, de alta criticidad o confidencial usando métodos de cifrado cuando sea necesario.

Todos los Servidores que utilizan computadores portátiles y equipos móviles, deberán estar alerta de los riesgos adicionales que se originan y los controles que se deberán implementar.

6.11 Trabajo remoto

El Equipo de Seguridad de Información deberá:

a) Realizar auditorías a los accesos de trabajo remoto periódicamente.

El Operador de Seguridad de Información en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

b) Autorizar la modalidad de trabajo remoto (desde fuera de las redes de la Corporación) siempre que en la Corporación se apliquen las disposiciones de seguridad y los controles establecidos.

c) Registrar en una bitácora las autorizaciones que se realicen y entregar mensualmente al Oficial de Seguridad de Información.

7 ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACION

7.1 Autorización para nuevos servicios de procesamiento de información

El responsable del área solicitante deberá:

a) Designar un responsable para un nuevo servicio a implementar.

b) Enviar una solicitud para la implementación de un nuevo servicio de procesamiento de información al Subdirector, Jefe o Responsable de TIC, con una descripción detallada conforme a las disposiciones vigentes relacionadas a adquisiciones y proyectos de TIC.

c) Autorizar explícitamente el uso de un nuevo servicio según las definiciones anteriores.

El Subdirector, Jefe o Responsable de Tecnologías de Información en coordinación con el Oficial de Seguridad de Información deberá:

d) Autorizar el uso del nuevo servicio garantizando el cumplimiento de la normativa de seguridad de la información.

e) Verificar que se ha realizado la evaluación de la compatibilidad a nivel de hardware y software con sistemas internos.

El Operador de Seguridad de Información en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

f) Implementar los controles necesarios para el uso de nuevos servicios para procesamiento de la información de la Corporación para evitar vulnerabilidades.

7.2 Análisis y especificaciones de los requerimientos de seguridad

El área de TIC deberá:

a) Analizar estrategias de desarrollo o compra del software de aplicación, así como el tratamiento que se dará a aquellos procesos de

emergencia que pudieran presentarse, de acuerdo a lo indicado en la "Guía de adquisición, desarrollo y mantenimiento".

El Operador de Seguridad de Información en conjunto con el área de TIC deberá:

b) Definir, identificar las especificaciones y requerimientos de seguridad, de acuerdo a solicitudes funcionales y técnicas, que serán evaluadas por el Oficial de Seguridad de Información.

El detalle sobre el análisis y especificaciones de los requerimientos de seguridad se encuentra en la "Guía de adquisición, desarrollo y mantenimiento de sistemas de información" adjunta a esta Norma Técnica.

7.3 Uso de controles criptográficos.

El Operador de Seguridad de Información en conjunto con el área de TIC deberá:

a) Implementar controles criptográficos cuando una aplicación tenga previsto el envío de mensajes que contengan información clasificada como reservada o confidencial, para lo cual se deberá:
   - Identificar el nivel requerido de protección de datos que se almacenará en el sistema, considerando: el tipo, fortaleza y calidad del algoritmo de cifrado (encriptación) requerido, a fin de proteger la confidencialidad, autenticidad e integridad de la información.
   - Analizar el uso de sistemas criptográficos para proteger la información sometida a riesgo, cuando otras medidas y controles no proporcionen la protección adecuada.

b) Proteger de claves cifradas (criptográficas).

c) Dar cumplimiento con el punto *Gestión de claves cifradas* de la "Guía de adquisición, desarrollo y mantenimiento" adjunto a esta Normas Técnica.

7.4 Gestión de cambios

El Operador de Seguridad de Información en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Definir y aplicar procesos de control de cambios para la implementación del software en el ambiente de producción, a fin de

minimizar el riesgo de alteración de los sistemas, sin que el programador o analista de desarrollo y mantenimiento de aplicaciones acceda a los ambientes de producción.

b) Definir un procedimiento que establezca los pasos para implementar las autorizaciones de paso a producción, a detalle, esta norma debe cumplirse mediante la "Guía de adquisición, desarrollo y mantenimiento", adjunto a esta Normas Técnica.

7.5 Protección de los datos de prueba del sistema

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Identificar por cada sistema, los datos que pueden ser copiados de un ambiente de producción a un ambiente de pruebas. El proceso de copiado de los Datos deberá ser realizado mediante un requerimiento por escrito que lo formalice.

b) Dar cumplimiento a la "Guía de adquisición desarrollo y mantenimiento" adjunto a esta Norma Técnica.

7.6 Control de acceso al código fuente de los programas

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Asignar a un Administrador de programas fuentes, que será el custodio y deberá: cumplir con determinadas actividades, relacionadas al acceso del código fuente de los programas.

b) Dar cumplimiento a la "Guía de adquisición, desarrollo y mantenimiento" adjunto a esta Norma Técnica.

7.7 Fuga de información

El Equipo de Seguridad de Información en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Realizar un monitoreo regular de las actividades del personal y del sistema, uso de los recursos en los sistemas de computador y transmisión de datos por la red; a fin de tomar acciones preventivas contra ataques, fuga de información, mal uso de activos de información

y demás riesgos que sobre los activos de información puedan presentarse.

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

b) Garantizar que un tercero no pueda deducir, extraer información de las comunicaciones, sistemas de modulación o de enmascaramiento, a partir de un comportamiento específico.

c) Restringir cuando sea posible y se considere necesario el envío de información a correos externos no institucionales.

d) Prevenir y restringir el acceso no autorizado a la red.

e) Examinar los códigos fuentes, cuando lo considere necesario, antes de utilizar los programas.

El Operador de Seguridad de Información deberá:

f) Explorar los medios y comunicaciones de salida para determinar la información oculta.

g) Controlar el acceso y las modificaciones al código instalado.

h) Utilizar herramientas para la protección contra la infección del software con código malicioso.

7.8 Desarrollo de software contratado externamente

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Definir acuerdos de licencias, acuerdos de uso, propiedad de código y derechos conferidos.

b) Definir los requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.

c) Definir procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.

d) Definir, cuando sea posible y se considere necesario, acuerdos de custodia de las fuentes del software o convenios de fideicomiso (y cualquier otra información requerida) en caso de quiebra de la tercera parte.

El Operador de Seguridad de Información deberá:

e) Verificar el cumplimiento de las condiciones de seguridad requeridas.

f) Realizar pruebas antes de la instalación para detectar códigos troyanos o maliciosos.

8 GESTION DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACION

8.1 Reporte sobre los eventos y debilidades de seguridad de la información

Todos los Servidores, contratistas y usuarios contratados por los proveedores deberán:

a) Tener conciencia de su responsabilidad para reportar todos los eventos de seguridad de la información. Bajo ninguna circunstancia, los Servidores deben intentar probar una debilidad sospechada o aplicar una solución a una vulnerabilidad por si solos.

b) Dar cumplimiento a la “Guía de gestión de incidentes de seguridad de información” adjunto a esta Norma Técnica.

El equipo de Seguridad de Información deberá:

c) Coordinar que los mecanismos de reporte deberán ser de fácil uso y acceso y deberán estar siempre disponibles.

8.2 Responsabilidades y procedimientos en Incidentes de Seguridad de Información.

a) El Operador de Seguridad de Información en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control, deberá planificar e implementar acciones correctivas para evitar la recurrencia de un incidente.

b) El Operador de Seguridad de Información deberá notificar al Oficial de

Seguridad de Información sobre la restauración del equipo, sistema o servicio afectado, una vez esté solucionado el incidente.

c) El Oficial de Seguridad de Información, en coordinación con el Subdirector de TIC, emitirá un reporte a los jefes de las áreas afectadas por el incidente e informará a la Corporación sobre el restablecimiento del servicio y/o sistema.

8.3 Aprendizaje debido a los incidentes de seguridad de la información

a) El equipo de Seguridad de Información deberá utilizar, para identificar los incidentes recurrentes o de alto impacto, la información que se obtiene de la evaluación de los incidentes de seguridad .

8.4 Recolección de evidencias

a) El Oficial de Seguridad de Información en conjunto con el área Jurídica y el de Talento Humano, según sea el caso, deberá desarrollar y cumplir procedimientos internos cuando se recolecta y se presenta evidencia con propósitos de acción disciplinaria dentro de la Corporación de acuerdo a lo establecido en el Reglamento Interno de Trabajo.

b) El Operador de seguridad deberá asegurar que los sistemas de información cumplan con las normas legales para la producción de evidencia.

c) Todos los Servidores deberán dar cumplimiento a la “Guía de gestión de incidentes de la seguridad de información” adjunta a esta Norma Técnica.

9 GESTION DE LA CONTINUIDAD DEL NEGOCIO

El alcance de todos los puntos de este título está enmarcado en la gestión adecuada de la seguridad de información en los sistemas informáticos, en el ambiente tecnológico y de comunicaciones de la Corporación y los procesos que reciben y producen información; es decir, en todos los activos de información de CELEC EP.

9.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

El Oficial de Seguridad de Información, en conjunto con Equipo de Seguridad de Información deberá:

a) Supervisar el proceso de elaboración e implantación del plan de continuidad y de recuperación de desastres, así como de la seguridad del personal.

b) Crear en conjunto con los propietarios de los activos de información y el área de Procesos, los procedimientos necesarios para garantizar la continuidad del negocio en la Corporación.

c) Someter a pruebas el plan de contingencias, así como también, controlar que existan entrenamientos y evaluaciones periódicas, o cuando se haya efectuado algún cambio en la configuración de los servicios, sistemas, equipos o el esquema de procesamiento.

d) El Oficial de Seguridad de Información deberá aprobar los planes de continuidad y recuperación de desastres informáticos y verificar que estén alineados a los planes corporativos.

El Operador de Seguridad de Información, en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control, deberá:

e) Identificar los activos involucrados en los procesos críticos de los servicios informáticos, de acuerdo "Guía de Gestión de Activos de Información", así como de los controles preventivos y mitigantes que pueden ser aplicados.

f) Elaborar la guía que permita mantener la continuidad de los servicios informáticos a su cargo, determinando los objetivos y el alcance del plan, mismo que será de carácter confidencial.

g) Elaborar un plan de recuperación de desastres de los servicios informáticos a su cargo, el mismo que comprenderá:
    - Actividades previas al desastre (bitácora de operaciones)
    - Actividades durante el desastre (plan de emergencias, entrenamiento)
    - Actividades después del desastre

9.2 Continuidad del negocio y evaluación de riesgos

El Oficial de Seguridad de Información, en coordinación con el área de TIC y/o

Administradores de Sistemas de Centros de Operación y Control deberá:

a) Analizar los riesgos, identificando las amenazas sobre los activos y su probabilidad de ocurrencia.

b) Analizar las vulnerabilidades asociadas a cada activo y el impacto que puedan provocar sobre la disponibilidad.

c) Obtener un mapa o matriz de riesgos que permita identificar y priorizar aquellos que pueden provocar una paralización de las actividades de la Corporación.

d) Crear una estrategia de gestión de control de riesgos y el plan de acción.

El Subdirector de TIC deberá:

e) Identificar, en conjunto con los Jefes área de TIC, los eventos que pueden ocasionar interrupciones en los proceso del negocio.

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

f) Entender las complejidades e interrelaciones existentes entre equipamiento, personas, tareas, departamentos, mecanismos de comunicación y relaciones con proveedores externos, los cuales pueden prestar servicios críticos que deben ser considerados.

g) Identificar y valorar el impacto de las interrupciones de los procesos, aplicaciones y servicios de los servicios informáticos, para cuantificar y calificar los impactos y saber sus efectos.

h) Identificar el tiempo máximo de interrupción permitida para cada servicio o aplicación crítica.

9.3 Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información

El Oficial de Seguridad de Información, en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Definir los equipos para ejecución del plan, donde se destacan las funciones claves que serán realizadas por los responsables:
    - Responsables de respuestas a incidentes: analizan el impacto del incidente;

- Logística: responsable de reunir todos los medios para ayudar a la puesta en operación de las actividades;
- Recuperación: puesta en servicio de la infraestructura.

b) Difundir y capacitar al personal responsable en los conceptos que contemplan la continuidad de los servicios de TIC y Centros de Operación y Control.

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

c) Definir las Estrategias para:
   - Seleccionar los sitios alternos y de almacenamiento externo;
   - Duplicado de los registros tanto físicos como electrónicos;
   - Incorporar RAID en los discos de los servidores;
   - Duplicar el suministro eléctrico; en lugares críticos especificados.
   - Estrategia de reinicio de las actividades;
   - Contratos de mantenimiento preventivo y correctivo;
   - Estrategia adecuada de respaldos;
   - Velar por la contratación de seguros para los activos
   - Métodos, procedimientos y procesos para la recuperación de los servicios.

El Operador de Seguridad de Información, en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

d) Desarrollar los procedimientos indicando el objetivo y el alcance, considerando las actividades y los tiempos de recuperación.

El área de Abastecimientos deberá:

e) Garantizar que se contrate los seguros pertinentes para los activos de información.

9.4 Estructura para la planificación de la continuidad del negocio

El Oficial de Seguridad de Información, en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Mantener una sola estructura de planes continuidad del negocio, para asegurar la consistencia de los planes, identificando las prioridades para las pruebas y mantenimiento.

El Operador de Seguridad de Información, en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

b) Mantener los documentos de los procesos actualizados, utilizando la gestión de cambios.

c) Crear planes de respuesta a los incidentes.

d) Describir los procedimientos de respaldo para desplazar las actividades esenciales de los servicios informáticos o los servicios de soporte a lugares temporales alternos, y para devolver la operatividad de los procesos en los plazos establecidos.

e) Describir los procedimientos de reanudación con las acciones a realizar para que las operaciones de los equipos y servicios vuelvan a la normalidad.

f) Definir los activos y recursos necesarios para ejecutar los procedimientos de emergencia, respaldo y reanudación de los servicios.

9.5 Pruebas, mantenimiento y revisión de los planes de continuidad del negocio

El Equipo de Seguridad deberá:

a) Realizar auditorías tanto internas como externas, identificando el tipo y alcance de la auditoría a realizar, entregando el plan de medidas correctivas para llevar a cabo las recomendaciones acordadas.

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

b) Ejecutar auto-evaluaciones del plan de continuidad, estrategias y procesos generados.

El Operador de Seguridad de Información, en conjunto con el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

c) Evaluar la capacidad de respuesta ante desastres verificando los tiempos de respuesta, validez de los procedimientos y capacidad de los responsables. Los resultados obtenidos permitirá actualizar y mantener los planes establecidos.

10 CUMPLIMIENTO

10.1 Identificación de la legislación aplicable

a) El Área Jurídica, deberá inventariar todas las normas legales, estatutarias, reglamentarias y contractuales pertinentes para los programas de software, servicio informático y en general todo activo de información que utiliza la Corporación.

b) El Oficial de Seguridad en conjunto con el Área Jurídica, deberá organizar para cada tipo de activo de información las normas legales, estatutarias, reglamentarias y contractuales pertinentes.

10.2 Derechos de Propiedad Intelectual

a) Los derechos de autor del software desarrollado a la medida pertenecerán a la Corporación y serán registrados en el organismo competente. Para el caso de software adquirido se obtendrá las respectivas licencias de uso.

b) Los Servidores, deberán cumplir los términos y condiciones de uso para el software desarrollado y la información, obtenidos de la Internet o proveedores (programas freeware, shareware, demostraciones o programas para pruebas). Deben utilizar solo software desarrollado, provisto o aprobado por el Subdirector de Tecnologías de la Información y Comunicaciones y/o por el Oficial de Seguridad de Información para la Corporación.

c) En los contratos realizados con terceros para desarrollo de software deberá constar que los derechos de autor será de la entidad contratante y el contratista entregará el código fuente.

El Oficial de Seguridad de Información, en conjunto con el área de TIC deberá:

a) Implementar procedimientos apropiados que permitan a la Corporación asegurar el cumplimiento de los requisitos legales al uso de derechos de propiedad intelectual y software patentado, aplicado tanto al software libre como al software propietario.

b) Implementar mecanismos para concienciar sobre las políticas para proteger derechos de propiedad intelectual y las acciones disciplinarias para el personal que las viole.

c) Controlar que no se duplique, convierta en otro formato, ni extraiga contenidos de grabaciones de audio y video, si no está expresamente

permitido por su autor o la persona que tenga los derechos sobre el material.

El Equipo de Seguridad de Información, en conjunto con el área de TIC deberá:

d) Mantener registros apropiados de los activos de información para proteger los derechos de propiedad intelectual. Se aplica tanto al software libre como al propietario.

e) Establecer una licencia pública general (GNU por sus siglas en inglés) al software desarrollado por la Corporación o contratado a terceros como desarrollo.

El área de TIC deberá:

f) Adquirir software que cubra las necesidades de la Corporación, únicamente a proveedores reconocidos para garantizar que no se violen derechos de propiedad intelectual.

g) Custodiar evidencia de la propiedad de licencias o suscripciones, contratos, discos maestros, manuales y toda la información relevante del software que se utiliza.

h) Controlar y asegurar que no se exceda el número máximo de usuarios permitidos para un programa de software libre o propietario.

i) Verificar que se instale únicamente software autorizado y con las respectivas licencias en el caso de utilizar software privativo.

j) Controlar que no se copie total ni parcialmente software privativo, códigos fuente y la documentación de programas de software con derechos de propiedad intelectual. Se exceptúa los programas de software libre bajo los términos de sus licencias públicas.

10.3 Protección de registros en cada Departamento

El Oficial de Seguridad de Información, en conjunto con el Equipo de Seguridad deberá:

a) Establecer y difundir en la entidad las directrices sobre retención, almacenamiento, manipulación y eliminación de registros e información.

El Equipo Seguridad de Información, en conjunto con el área de TIC deberá:

b) Establecer procedimientos para revisar el nivel de deterioro de los medios utilizados para almacenamiento, garantizar el acceso a los datos e información registrada, tanto el medio como el formato, durante todo el periodo de retención.

c) Establecer un procedimiento para cambiar o actualizar la tecnología del medio en el cual se almacenan los activos de información y registros de acuerdo a las innovaciones tecnológicas disponibles en el mercado.

d) Inventariar las fuentes de información clave.

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

e) Mantener la documentación y especificaciones técnicas de los algoritmos y programas utilizados para el cifrado y descifrado de archivos y toda la información relevante relacionada con claves, archivos criptográficos o firmas electrónicas, para permitir el descifrado de los registros durante el periodo de tiempo para el cual se retienen.

f) Seleccionar los sistemas de almacenamiento de manera que los datos requeridos se puedan recuperar en el periodo de tiempo y en formatos legibles, dependiendo de los requisitos que se deben cumplir.

g) Garantizar la identificación de los registros y el periodo de retención de los mismos tal como se defina en normas legales ecuatorianas. Este sistema debe permitir la destrucción adecuada de los registros después de este periodo, si la entidad no los necesita y las normas así lo especifican.

h) Implementar controles apropiados para proteger los registros contra pérdida, destrucción y falsificación de la información. Utilizar como referencia para la gestión de los registros de la Corporación la norma ISO 15489-1 o su homóloga ecuatoriana.

El Operador de Seguridad de Información, en conjunto con el Responsable del activo de información deberá:

i) Clasificar los registros electrónicos y físicos por tipos, especificando los periodos de retención y los medios de almacenamiento, como discos, cintas, entre otros.

j) Implementar según las recomendaciones del fabricante, procedimientos de manipulación y almacenamiento.

10.4 Protección de los datos y privacidad de la información personal

De acuerdo a la normativa legal vigente prima el principio que los datos personales pertenecen a las personas y no a las instituciones.

a) El Oficial de Seguridad de la Información deberá garantizar la existencia de controles para la protección de datos y privacidad de la información personal, de acuerdo a la legislación aplicable.

El Operador de Seguridad de Información, en conjunto con el área de TIC, deberá:

b) Implementar controles apropiados para gestionar el acceso a la información personal, de acuerdo con la legislación aplicable.

c) Implementar mecanismos de carácter organizacional y tecnológico para autorización al acceso, uso e intercambio de datos personales de las personas o ciudadanos en custodia de las entidades públicas.

10.5 Prevención del uso inadecuado de servicios de procesamiento de información

El Oficial de Seguridad de Información, en conjunto con el Subdirector de TIC deberá:

a) Definir la política para autorización de uso de los servicios de procesamiento de información aprobados, misma que debe ser suscrita por cada Servidor en relación de trabajo permanente o temporal, así como contratistas, asesores, proveedores y representantes de terceras partes.

El Equipo de Seguridad de Información deberá:

b) Implementar mecanismos para identificar el uso inadecuado de los servicios por medio de monitoreo u otros medios.

c) Definir y especificar en las normas internas, las acciones legales o disciplinarias cuando se compruebe el uso no adecuado de los servicios de procesamiento de información.

d) Implementar mecanismos tecnológicos y organizacionales para detectar la intrusión y evitar el uso inadecuado de los servicios de procesamiento de información.

El Subdirector de TIC deberá:

e) Definir y comunicar los servicios de procesamiento de información aprobados, así como los criterios para establecer el uso de estos servicios para propósitos no relacionados con la entidad sin autorización de la Gerencia General, o para cualquier propósito no autorizado.

El Operador de Seguridad de Información, en conjunto con el área de TIC deberá:

f) Implementar en los servicios de procesamiento de información que sea posible, el mensaje de advertencia que indique que el servicio al cual se está ingresando es propiedad de la entidad 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. El uso de los servicios de procesamiento de información de la entidad tendrán como fin principal o exclusivo los asuntos de la Corporación y no los personales o de otra índole.

10.6 Controles criptográficos

El Operador de Seguridad de Información, en conjunto con el área de TIC y el Especialista en Criptografía del Equipo de Seguridad, deberá:

a) Controlar la adquisición e implementación de hardware y software de computadores a ser usados para la ejecución de funciones criptográficas; o diseñados para adicionarles funciones criptográficas.

b) Controlar el uso de encriptación, y especificar y documentar los ámbitos en dónde se aplicarán tales procesos (ej., comunicaciones, firma de documentos, trasmisión de datos, entre otros).

c) Garantizar el cumplimiento con las leyes y los reglamentos nacionales antes de desplazar información encriptada o controles criptográficos a otros países.

10.7 Cumplimiento de las normas de seguridad de información

El Oficial de Seguridad, con el apoyo del Equipo de Seguridad de Información coordinará:

a) Revisar en intervalos regulares reportes e informes de seguridad de los sistemas de información procesamiento de información de acuerdo con la política de la seguridad, las normas y cualquier otro requisito de seguridad.

b) Auditar las plataformas técnicas y los sistemas de información para determinar el cumplimiento de las normas aplicables sobre implementación de la seguridad y sus controles.

c) Registrar y conservar los resultados de las revisiones y las acciones correctivas llevadas a cabo por la dirección.

d) Verificar el cumplimiento técnico a través de: herramientas de software o hardware, de manera manualmente o automatizada; esta actividad, debe contar con el apoyo de profesionales con experiencia técnica especializada de acuerdo al área.

e) Aplicar evaluaciones de vulnerabilidad o pruebas de penetración considerando siempre el riesgo de que dichas actividades pueden poner en peligro la seguridad del sistema. Tales pruebas se deberán planificar, documentar y ser repetibles dentro del período previamente establecido.

f) Controlar que la verificación del cumplimiento técnico sea realizado por personas autorizadas y competentes o bajo la supervisión de dichas personas.

g) Analizar los sistemas operativos para asegurar que los controles de hardware y software se han implementado correctamente.

h) Ejecutar o contratar pruebas de penetración y evaluaciones de la vulnerabilidad, las cuales deben ser realizadas por expertos independientes especialmente contratados para este propósito.

El Subdirector, los Jefes y/o Responsables del área de TIC, deberán informar de los resultados a las personas que realizan revisiones independientes, cuando la revisión tiene lugar en el área de competencia.

10.8 Controles de auditoría de los sistemas de información

El Oficial de Seguridad, deberá dar cumplimiento a:

a) Salvaguardar los servicios de procesamiento de información y las herramientas de auditoría durante las auditorías de los sistemas de información.

b) Proteger la integridad y evitar el uso inadecuado de las herramientas de auditoría.

c) Acordar los requisitos así como el alcance de las auditorías con el área correspondiente.

d) Dar a los auditores únicamente acceso de lectura a la información. Identificar y acordar los requisitos para el procesamiento especial o adicional.

e) Monitorear y registrar los accesos, cuando sea posible, para crear un rastreo para referencia. El uso de rastreos de referencia de tiempo se debe considerar para datos o sistemas críticos.

f) Documentar todos los procedimientos, requisitos y responsabilidades de la auditoría.

g) Asegurar que la persona que realiza la auditoría sea independiente de las actividades auditadas.

h) Identificar explícitamente y poner en disposición los recursos correspondientes, para llevar a cabo las auditorías.

10.9 Protección de las herramientas de auditoría de los sistemas de información

El Equipo de Seguridad de Información en conjunto con el Operador de Seguridad de Información, deberá:

a) Instalar y administrar las herramientas de auditoría.

b) Implementar controles para separar los programas de software o archivos de datos de auditoría, de los sistemas de información y de desarrollo de la Corporación.

c) Implementar controles para la protección de manipulación de los archivos de seguridad y auditoría que generan los sistemas de procesamiento de información.

d) Mantener un estricto control de respaldos y tiempo de retención de los archivos de seguridad y auditoría de acuerdo al tipo de información y la política que se defina.

e) Mantener archivos de seguridad y auditoría en librerías de cinta, siempre que se les proporcione un nivel adecuado de protección

adicional.

f) Bloquear el acceso a los archivos de seguridad y auditoría a los Servidores no autorizados y de acuerdo al procedimiento que se defina.

GLOSARIO DE TÉRMINOS

- **Activo**: Todo bien que tiene valor para la Corporación.
- **Activo de Información**: Es todo aquel elemento que compone el proceso de la comunicación o flujo de información, partiendo desde la información como tal, su emisor, el medio por el cual se transmite, hasta su receptor. Se los separa en tres categorías básicas:
    - Personal Información Equipos que soportan dicha información
    - Software
    - Hardware
    - Infraestructura física y redes de transmisión de energía e información
    - Infraestructura lógica

  Los activos son elementos que la seguridad de la información busca proteger. Los activos poseen valor para las empresas y como consecuencia de ello, necesitan recibir una protección adecuada para que sus negocios no sean perjudicados.
- **Administración de Riesgos**: También conocido como Gestión de Riesgos, es el proceso de identificación, control y minimización o eliminación, a un costo aceptable, que incluye la identificación de riesgos, medidas reductoras de riesgos y el impacto del presupuesto en cuanto a la implementación de decisiones relacionadas a la aceptación, evitación o transferencia del riesgo. Además incluye el proceso de asignación de prioridades a la creación de presupuesto, implementación y mantenimiento apropiado de las medidas reductoras de riesgos. La administración de riesgos es un proceso continuo de complejidad creciente. Es como se evalúa el impacto de exposiciones y las respuestas a ellas.
- **Ambiente de Desarrollo**: tiene las siguientes características:
    - En este ambiente se desarrollan los programas fuentes se almacena toda la información relacionada con el análisis y diseño de los sistemas.
    - El analista o programador (desarrollador) tiene total dominio sobre el ambiente, y puede instalar componentes o actualizar versiones del software base.
    - Todos los cambios del código, de software base y de componentes deben ser debidamente documentados.
    - Se registra en el sistema el control de versiones que administra el "Administrador de programas fuentes".
    - El desarrollador realiza las pruebas con los datos de la base de datos desarrollo.
    - Cuando se considera que el programa está terminado, se lo pasa al ambiente de pruebas junto con la documentación requerida que se le entregará al implementador de ese ambiente.
- **Ambiente de Pruebas**: tiene las siguientes características:
    - Este ambiente es utilizado para realizar pruebas previas al paso a

producción.
- Deberá disponer del mismo software base que el ambiente producción.
- El implementador de este ambiente recibe el programa y la documentación respectiva y realiza una prueba general con un lote de datos para tal efecto.
- Las pruebas se realizan con los datos de la base de datos de pruebas. Si no se detectan errores de ejecución, los resultados de las rutinas de seguridad son correctas de acuerdo a las especificaciones y se considera que la documentación presentada es completa, entonces se emite un informe favorable y se pasa el programa fuente al implementador de producción por medio del sistema de control de versiones y se le entrega las instrucciones. Caso contrario, vuelve atrás el ciclo devolviendo el programa al desarrollador, junto con un detalle de las observaciones.

- **Ambiente de Capacitación**: tiene las siguientes características:
  - Este ambiente es idéntico al ambiente de producción en su estructura, versiones de sistema y software base.
  - Este ambiente será utilizado para realizar las capacitaciones respectivas a los usuarios de los sistemas.
  - Este ambiente no se actualizará con la información de producción para realizar pruebas.
  - Este ambiente también debe ser considerado para los respaldos de datos.
- **Ambiente de Producción**: tiene las siguientes características:
  - Es donde se ejecutan los sistemas y se encuentran los datos productivos.
  - Los programas fuentes certificados se guardan en un repositorio de fuentes de producción, almacenándolos mediante un sistema de control de versiones que maneja el "administrador de programas fuentes" y donde se registran los datos del programador que hizo la modificación, fecha, hora y tamaño de los programas fuentes y objetos o ejecutables.
  - El "implementador" compila el programa fuente dentro del ambiente de producción, asegurando que hay una correspondencia biunívoca con el ejecutable en producción y luego (este fuente) se elimina, dejándolo en el repositorio de programas fuentes.
  - Procedimientos de la misma naturaleza que el anterior, deberán aplicarse para las modificaciones de cualquier otro elemento que forme parte del sistema; por ejemplo: modelo de datos de la base de datos o cambios en los parámetros, etc. Las modificaciones realizadas al software de base (Sistemas Operativos, Motores de bases de datos, software middleware) deberán cumplir idénticos pasos, sólo que las implementaciones las realizarán los propios administradores.
  - El personal de desarrollo, como el proveedor de los aplicativos, no

deben tener acceso al ambiente de producción, así como tampoco a los datos reales para la realización de las pruebas en el Ambiente de Prueba. Para casos excepcionales, se debe documentar adecuadamente la autorización, los trabajos realizados y monitorearlos en todo momento.

- **Área de TIC:** Se toma al área de Telecomunicaciones encargada de los servicios del SNI y áreas relacionadas con la administración de Sistemas del Núcleo de Negocio, como parte del área de Tecnologías de la Información y Comunicaciones. Al hablar del "área de TIC" se entiende además a todas las áreas de TIC de la Corporación y a la Subdirección de TIC de Matriz. Se entiende que dentro del área de TIC existen varios responsables técnicos de las tareas asignadas a ésta área en el presente documento.
- **Autenticidad**: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Autorización**: Acto administrativo a través del cual se le otorga permiso a un usuario para acceder a los datos, funcionalidad o servicio de un sistema en particular.
- **Capacidad de Auditoría**: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- **Ciberseguridad:** conjunto de tecnologías, procesos, procedimientos y servicios encaminados a la protección de los activos sean estos físicos, lógicos o de servicios, que dependan en alguna medida de un soporte TIC.
- **Ciberseguridad Industrial:** comprende la prevención, monitorización y mejora de la resistencia de los sistemas industriales y su recuperación, ante acciones inesperadas que puedan afectar el correcto funcionamiento de los procesos industriales.
- **Clave**: Mecanismo de seguridad que permite validar el ingreso de un usuario a un recurso evitando que sean utilizados por personas no autorizadas.
- **Código móvil**: Software transferido entre sistemas, ya sea a través de una red u otros medios, que se ejecuta en el sistema local sin la instalación explícita del mismo por parte de un usuario.
- **Comité de Gestión de Seguridad de la Información**: Equipo integrado por los tomadores de decisión de la Corporación. Se encarga de autorizar cambios en las políticas de Seguridad, proyectos grandes de Seguridad de Información y deciden como actual en tiempos de crisis de Seguridad.
- **Confiabilidad de la Información**: La información generada debe ser adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- **Confidencialidad**: Garantizar que la información sea accesible sólo a aquellas personas, recursos y/o procesos autorizados a tener acceso a la misma.
- **Corporación**: En este documento y en las Guías que lo acompañan se denomina así a la Empresa Pública Estratégica Corporación Eléctrica del

Ecuador CELEC EP.

- **Disponibilidad**: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
- **Equipo de Seguridad de Información**: Es un cuerpo integrado por representantes expertos en el negocio y en los procesos de todas las áreas de la Corporación, cuya labor primordial es salvaguardar los Activos de Información y garantizar su Confidencialidad, Disponibilidad e Integridad, mediante el apoyo manifiesto de las autoridades a las iniciativas de seguridad.
- **Encriptar:** Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que solo pueda leerlo la persona que cuente con la calve de cifrado adecuada para decodificarlo.
- **Evaluación de Riesgos**: Evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operación de la Corporación.
- **Grupos de interés**: Asociaciones, comisiones, proyectos, institutos de normalización, esquemas, cuyo objeto es la seguridad de información o temas relacionados.
- **Incidente de Seguridad**: Un incidente de seguridad es un evento que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de los activos de información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.
- **Información**: Es uno de los activos más importantes de las instituciones, en las formas que esta se manifieste: textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, magnético, papel, electrónico, computadoras, audiovisual y otros.
- **Integridad**: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento. Es la protección de los activos de información de cambios no autorizados, ya sean intencionales o accidentales.
- **No repudio**: se refiere eliminar la capacidad de qué entidad, usuario, recurso y/o proceso que haya participado en una transacción, alegue ante terceros que no lo hizo.
- **Legalidad**: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones empresariales, nacionales o internacionales.
- **Licencia pública general:** La Licencia Pública General de GNU o más conocida por su nombre en inglés GNU General Public License (o simplemente sus siglas del inglés GNU GPL) es la licencia más ampliamente usada en el mundo del software y garantiza a los usuarios finales (personas, organizaciones, compañías) la libertad de usar, estudiar, compartir (copiar) y modificar el software.
- **Oficial de Segundad de la Información**: Es el responsable de coordinar

las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento del Programa de Seguridad de la Información. Es la persona que cumple la función de supervisar el cumplimiento de la presente Norma Técnica y de asesorar en materia de seguridad de la información a los integrantes de la Corporación que así lo requieran. Es también, la persona responsable de planear, coordinar y administrar los procesos de seguridad de información en la Corporación, incluyendo la estrategia Corporativa.

- **Programa de Seguridad de Información**: Es el conjunto de actividades y proyectos de Seguridad de Información que se realizan en la Corporación y que comprende la evaluación, diseño, implementación y operación de controles, de Seguridad de Información tanto en procesos de apoyo como del núcleo de negocio.
- **Propietarios de la Información**: Son los responsables de clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.
- **Protección a la duplicación**: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- **Responsables de la información:** Son los Servidores a cargo del uso, edición y mantenimiento de los activos de información.
- **Responsable del Área de Recursos Humanos**: Cumplirá la función de comunicar a todo el personal que ingresa, de sus obligaciones respecto del cumplimiento del Programa de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de él surjan. Asimismo, tendrá a su cargo, la difusión del presente documento a todo el personal, de los cambios que en ella se produzcan, de la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y de las tareas de capacitación continua en materia de seguridad en coordinación con el Oficial de Seguridad de la información.
- **Responsable del Área de Tecnologías de la Información**: (Operador de Seguridad de Información) Cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la Corporación. Por otra parte, tendrá la función de supervisar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.
- **Responsable del Área Legal**: Verificará el cumplimiento del Programa de Seguridad de la Información en la gestión de todos los contratos, acuerdos u otra documentación de la Corporación con sus Servidores y con terceros. Asimismo, asesorará en materia legal a la Corporación, en lo que se refiere a la seguridad de la información.

- **Seguridad de la Información**: La seguridad de la información se entiende como la preservación de los siguientes principios aplicables a los activos de información: Confidencialidad, Integridad y Disponibilidad.
- **Servidor**: Persona que mantiene una relación laboral de dependencia con la Corporación. Siempre que se haga alusión a una persona se escribirá con "**S**" mayúscula**.**
- **servidor:** Equipo de computación en el cual se procesan y/o almacenan datos. Siempre que se hable de equipos de hardware se escribirá con "**s**" minúscula.
- **Sistema de Información**: Se refiere a un conjunto de recursos de TIC organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
- **SIN:** Sistema Nacional Interconectado.
- **Tecnología de Información y Comunicaciones (TIC)**: Se utiliza para referirse a los Departamentos y Subdirección de Tecnología de Información y Comunicaciones de CELEC EP. Se refiere también, al hardware, software y redes de datos operados por la Corporación o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la Corporación.
- **Terceros**: Son todas aquellas personas naturales o jurídicas, que no forman parte de la Corporación, por ejemplo: contratistas, oferentes, clientes, proveedores.
- **Usuario**: Se considera usuario a cualquier Servidor de la Corporación, tanto interno como externo, a quien se le haya proporcionado una cuenta de dominio, utilice el servicio de correo electrónico o se le otorgue accesos a la red interna u otros sistemas de la CELEC EP.

Sección II

Instructivo de Aplicación

SIC-INS-001-2014

Revisión 1

Diciembre - 2014

CONTENIDO

INTRODUCCIÓN

La Empresa Pública Estratégica Corporación Eléctrica del Ecuador CELEC EP, mediante Resolución de Gerencia General, Memorandos internos y Oficios, ha designado al Oficial de Seguridad de Información y ha constituido el Equipo de Seguridad de Información para la Corporación.

El Equipo de Seguridad, tomando en cuenta las necesidades de la corporación y basándose en las normas ISO27000:2013, NTE-INEN 27000 y los estándares NERC-CIP, ha creado las Normas Técnicas de Seguridad de Información (SIC-NTE-001-2014) y las Guías que la acompañan.

En el contexto anterior, se emite este Instructivo que explica el mapa de ruta de implementación de controles, el esquema de seguimiento y otros criterios a tomar en cuenta para la aplicación de estas Normas y sus Guías.

ALCANCE

Este documento aplica para las Normas Técnicas de Seguridad de Información (SIC-NTE-001-2014) y las Guías de la Norma Técnica, las mismas que hasta el momento son:

- Control de acceso SIC-GCA-001-2014
- Contratos y compromiso de confidencialidad SIC-GLG-001-2014
- Guía rápida para usuarios SIC-GLG-002-2014
- Gestión de activos de información SIC-GAI-001-2014
- Gestión del cambio cultural SIC-GRH-001-2014
- Gestión de incidentes de seguridad de información SIC-GIS-001-2014
- Adquisición, desarrollo y mantenimiento de sistemas de Información SIC-GMS-001-2014

OBJETIVO

Explicar el mapa de ruta de implementación de controles, esquema de seguimiento y otros criterios a tomar en cuenta para la aplicación de las citadas Normas y Guías, en la Corporación.

1 DATOS GENERALES

1.1 Identificación de documentos

Las Normas Técnicas y Guías se encuentran codificadas con un identificador que contiene 4 grupos de 3 caracteres.

A manera de ejemplo, tomaremos el código de este instructivo **SIC-INS-001-2014**:

1. SIC: Seguridad de Información Corporativa
2. INS: Identificador del tipo de documento
    a. POL: Política
    b. NTE: Norma técnica
    c. GXX: Guía. Las últimas dos letras de este grupo corresponden al dominio de seguridad de información al que aplica la guía. Por ejemplo, **GIS** corresponde a la guía de **G**estión de **I**ncidentes de **S**eguridad.
    d. INS: Instructivo
3. 001: Número secuencial del documento dentro de su tipo.
4. 2014: Año en el que el documento fue creado.

1.2 Validez de documentos

Tanto las Normas como las Guías y el presente instructivo tienen validez desde su emisión hasta que sean formalmente reemplazados por una nueva versión o eliminados por la máxima autoridad de la Corporación o el Oficial de Seguridad de Información Corporativa.

La fecha de emisión se encuentra claramente especificada en la página 2 de los documentos, indicando además los responsables de su revisión y aprobación.

2 CONTENIDO

Los documentos normativos de Seguridad de Información para la Corporación, hasta el momento, son que se explican en esta sección. A medida que se vayan generando nuevos documentos, este instructivo será actualizado y serán socializados a todo el personal.

2.1 SIC-NTE-001-2014

Norma Técnica de Seguridad de Información. Contiene las definiciones técnicas de seguridad de información que se deben aplicar a los activos de información de la Corporación y a los controles que los salvaguardan.

La Norma Técnica contiene los siguientes dominios de seguridad:

1. **Lineamientos generales:** Muestra la distribución de responsabilidades sobre seguridad de información dentro de la Corporación, así como otros lineamientos generales en cuanto a comunicación, acuerdos con terceros y auditorías.
2. **Gestión de activos:** Define las reglas para el uso aceptable y responsable, así como también las directrices de clasificación y etiquetado del inventario de activos de información.
3. **Seguridad de los recursos humanos:** Muestra lo que se debe hacer en procesos de selección, define funciones y responsabilidades, retiro de privilegios y trata también sobre la sensibilización de la seguridad de información en la Corporación.
4. **Seguridad física y del entorno:** Explica que controles se deben considerar y disponer para proteger las localidades donde están presentes los activos de información.
5. **Gestión de comunicaciones y operaciones:** Abarca todos los aspectos concernientes a la operación de Sistemas de Información, incluyendo la gestión de vacíos, separación de ambientes, transacciones en línea, sincronización de datos, implementación de controles para activos de información, entre otros.
6. **Control de acceso:** En este capítulo se hablan sobre privilegios de usuarios, propietarios de la información, identificación de Servidores dentro de un sistema, control de conexiones y protección de todo tipo de medios de acceso a activos de información.
7. **Adquisición, desarrollo y mantenimiento de sistemas de información:** Como su nombre lo indica, describe los controles que se deben tener al momento de contratar el desarrollo de aplicaciones o módulos de las mismas. Este mismo concepto aplica a las solicitudes de cambio en los sistemas existentes en la Corporación.
8. **Gestión de los incidentes de la seguridad de información:** Se describe la manera de reportar eventos y debilidades de seguridad de información, las responsabilidades de todos los miembros de la cadena de custodia de un activo de información, recolección de evidencias, entre otros temas.
9. **Gestión de la continuidad del negocio:** Define el marco sobre el cual se debe actuar para la generación de planes de continuidad y contingencia para los activos críticos de infraestructura y los activos de información.
10. **Cumplimiento:** Informa sobre el marco legal, la aplicación y la verificación del cumplimiento de la Norma Técnica y sus Guías.

11. **Glosario de términos:** Muestra una lista con definiciones de términos técnicos del campo de seguridad de información. Este glosario es complementado con los existentes en las Guías.

2.2 SIC-GMS-001-2014

La ***Guía de adquisición, desarrollo y mantenimiento de sistemas de Información***, establece los criterios que los sistemas de información de la Corporación deben cumplir previo a su adquisición o durante su desarrollo y mantenimiento.

2.3 SIC-GCA-001-2014

La ***Guía de control de acceso***, establece una metodología para la identificación y autenticación de usuarios, evitando comprometer la seguridad los servicios que sustentan los activos de información de la Corporación.

2.4 SIC-GLG-001-2014

La ***Guía de contratos y compromiso de confidencialidad***, corresponde a lineamientos generales y busca responsabilizar y concientizar al funcionario sobre el buen uso de los activos de información. Se establecen además lineamientos para garantizar la integridad, disponibilidad y confiabilidad de la información; y, un compromiso de confidencialidad que deberá ser firmado por todos los Servidores de la Corporación.

2.5 SIC-GLG-002-2014

La ***Guía rápida para usuarios***, constituye un resumen de los puntos clave de la Norma Técnica de Seguridad de Información que todo Servidor debería conocer.

2.6 SIC-GIS-001-2014

La ***Guía de gestión de incidentes de seguridad de información***, establece los lineamientos para identificar y planificar de manera eficiente las acciones, canales de comunicación, responsabilidades y aplicación de controles mitigantes sobre los activos de información.

2.7 SIC-GAI-001-2014

La ***Guía de gestión de activos de información***, muestra las directrices para clasificar, definir responsables y valorar los activos de información.

2.8 SIC-GRH-001-2014

La ***Guía de gestión del cambio cultural***, muestra las estrategias para realizar programas de sensibilización, su evaluación y modificación.

3 APLICACIÓN

3.1 Definiciones generales

a) La Norma Técnica y sus Guías son de obligatoria aplicación en toda la Corporación y para todos los activos de información.
b) La aplicación de los controles y de las directivas que contienen los documentos de la Norma, cuando la tecnología, la documentación y los recursos lo permitan, debe ser inmediata) es decir, a partir de la aprobación del Gerente General y socialización.
c) Para las directrices para cuyo cumplimiento sea necesario realizar trabajos de más de 3 meses y que comprendan una inversión de recursos mayor al definido para ínfima cuantía, se las deberá aplicar de manera planificada y con coordinación previa con el Oficial de Seguridad de Información Corporativa.
d) El Oficial de Seguridad de Información aprobará las Guías y procedimientos que considere necesario para cubrir las necesidades de seguridad de información, bajo el marco de las Normas Técnicas de Seguridad de Información aprobadas por el Gerente General.
e) El Oficial y el Equipo de Seguridad de Información, se encargarán de monitorear el cumplimiento de ésta Norma Técnica y sus Guías, de tal forma que la disponibilidad, confidencialidad e integridad de los activos de información sea salvaguardada; para ello, brindarán el apoyo técnico necesario para que los controles se implementen de manera eficaz.

3.2 Definiciones especiales

Para los casos puntuales de mejora expuestos en el Informe de auditoría de estados financieros 2010-2011 detectados en los sistemas de información de la

Corporación, el cumplimiento de las recomendaciones y de los lineamientos existentes en la Norma Técnica y sus Guías será de la siguiente manera:

a) Todos los meses las áreas de Talento Humano verificarán con el personal que maneja los sistemas de información, que el personal que tiene acceso a ellos es estrictamente el de la nómina al momento de la verificación.
b) Todas las personas que ya no forman parte de la Corporación deberán ser desactivadas de todos los sistemas de información existentes en la Corporación (ya sean corporativos o de uso exclusivo de una Unidad de Negocio) hasta el 28 de Febrero de 2015.
c) Toda la información de los usuarios que conste en los sistemas de información existentes en la Corporación (ya sean corporativos o de uso exclusivo de una Unidad de Negocio) deberá estar actualizada hasta el 28 de Febrero de 2015, en especial el área y Unidad de Negocio a la que pertenecen.
d) Todos los usuarios genéricos existentes hasta la fecha de expedición de estas Normas Técnicas serán desactivados. Para restaurar su funcionamiento se deberá proceder conforme a lo estipulado en la Guía de Control de Accesos. .
e) Para el acceso a todos los sistemas de información existentes en la Corporación (ya sean corporativos o de uso exclusivo de una Unidad de Negocio), las claves de los usuarios deben estar configuradas de acuerdo a la Guía de Control de Accesos hasta el 28 de Febrero de 2014.
f) Para el acceso a todos los sistemas de información existentes en la Corporación (ya sean corporativos o de uso exclusivo de una Unidad de Negocio), los nombres de usuario deberán estar configurados de acuerdo a la Guía de Control de Accesos y además deberán validarse con el Directorio Activo corporativo (incluyendo los usuarios de los sistemas operativos) hasta el 31 de Julio de 2015. Si tecnológicamente no fuere posible, el Gerente de la Unidad de Negocios donde suceda este caso, deberá enviar un informe debidamente sustentado al Oficial de Seguridad de Información de la Corporación.
g) El plan de contingencias para los sistemas de información existentes en la Corporación (ya sean corporativos o de uso exclusivo de una Unidad de Negocio), debe ser diseñado, desarrollado, implementado y probado hasta el 31 de Diciembre de 2015.
h) Todos los accesos a los Centros de Datos existentes en la Corporación (ya sean corporativos o de uso exclusivo de una Unidad de Negocio) deben mantener una bitácora de registro de acceso al mismo, para personal externo e interno. Esta bitácora deberá implementarse hasta el 28 de Febrero de 2015.

4 CUMPLIMIENTO

Se verificará el cumplimiento de las definiciones (excepto las definiciones especiales de este instructivo) dentro de la Norma Técnica y las Guías, a partir del 01 de Agosto de 2015, por lo que desde la expedición de este instructivo hasta la fecha mencionada, el Equipo de Seguridad de Información trabajará en conjunto con las áreas pertinentes para la implementación de los controles correspondientes.

Para las definiciones del punto 3.2 de este instructivo, la verificación de su cumplimiento empezará a partir del día siguiente del plazo formulado.

Para los controles que, por alguna razón justificada no pudieran ser implementados hasta las fechas establecidas, el Oficial de Seguridad de Información trabajará en conjunto con las áreas responsables de la operación del control, en la elaboración de un plan de implementación.

Sección III

Guía de control de acceso

SIC-GCA-001-2014

Revisión 1

Diciembre - 2014

CONTENIDO

OBJETIVOS

- Establecer una metodología para la identificación y autentificación de usuarios, evitando comprometer la seguridad en todos los servicios que soportan los activos de información de la Corporación.
- Definir controles para impedir el acceso no autorizado a los sistemas de información, base de datos y servicios de información.
- Implementar controles en el acceso a sistemas utilizando métodos de autentificación y autorización que permitan registrar y revisar los eventos y actividades realizadas por parte de los usuarios.
- Concientizar a los Servidores del uso responsable de las contraseñas y equipos en CELEC EP.
- Definir responsabilidades para identificar, gestionar y mantener perfiles de los custodios de información.
- Definir claramente los autorizadores de los permisos de acceso a la información.
- Otorgar una identificación única a todos los usuarios internos, externos y temporales que interactúen con los activos de información de la Corporación.

ALCANCE

La "Guía de control de acceso" en la Empresa Pública Estratégica de la Corporación Eléctrica del Ecuador CELEC EP es de aplicación obligatoria en todas las dependencias y Servidores que conforman la Corporación.

1. RESPONSABILIDADES

- El Oficial de Seguridad es el responsable de proponer y solicitar aprobación de la emisión de la Norma Técnica y sus guías.
- El Gerente General, es quien aprueba y emite de las Normas Técnicas y Guías.
- Los Servidores de la Corporación, son responsables de la aplicación, cumplimiento y de la respectiva, Norma Técnica y sus Guías.

2. CONTROL DE ACCESO A LAS APLICACIONES Y A LA INFORMACIÓN

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberán:

a) Controlar el acceso de usuarios a la información y a las funciones del sistema de aplicación, de acuerdo con la política del sistema (que deberá seguir los documentos de Norma Técnica y sus Guías definidas para control de acceso);
b) Suministrar protección contra acceso no autorizado por un programa utilitario, software del sistema operativo, software malicioso o cualquier otro software que pueda anular o desviar los controles de seguridad del sistema;
c) Evitar poner en riesgo otros sistemas con los que se comparten los recursos de información.
d) La identificación de usuario es única e intransferible.
   El responsable de toda actividad realizada con este identificador responderá por cualquier acción realizada con éste.

2.1. Uso de las utilidades del sistema

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberán:

a) Restringir y controlar estrictamente el uso de programas utilitarios con los siguientes preceptos:
   - Usar procedimientos de identificación, autenticación y autorización para programas utilitarios.
   - Separar los programas utilitarios del software de aplicaciones.
   - Limitar el uso de programas utilitarios al mínimo y establecer tipos de usuarios autorizados para su uso.
   - Crear un proceso para la autorización del uso de programas utilitarios no estándares de la Corporación.
   - Establecer un límite de tiempo para el de uso de programa utilitarios.
   - Mantener un registro del uso de programas utilitarios.
   - Estableces un procedimiento para retiro o inhabilitación de todas los programas utilitarios innecesarios.

2.2. Tiempo de inactividad de la sesión

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberán:

a) Suspender las sesiones inactivas después del período definido en la política de accesos del sistema, sin consideración de lugar o dispositivo desde el cual se realice el acceso.
b) Parametrizar el tiempo de inactividad en los sistemas de procesamiento de información para suspender y cerrar sesiones.

2.3. Limitación del tiempo de conexión

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberán:

a) Utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo. Los siguientes son algunos ejemplos de estas restricciones:
    - Configurar espacios de tiempo predeterminados para procesos especiales (por ejemplo, transmisiones de datos o archivos, obtención de respaldos, mantenimientos programados, entre otros.)
    - Restringir los tiempos de conexión a las horas normales de oficina, si no se requiere tiempo extra u operaciones de horario prolongado;
    - Requerir la autenticación a intervalos determinados cuando lo amerite
    - Proporcionar accesos temporales para ciertas operaciones (por ejemplo, mediante tickets o tokens electrónicos temporales)

2.4. Relativo a la seguridad de las aplicaciones

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberán:

a) Autenticar usuarios autorizados, de acuerdo a esta Guía.
b) Llevar un registro de definición para el uso de privilegios especiales del sistema.
c) Utilizar mecanismos como: uso de dominios de autenticación, servidores de control de acceso y directorios.
d) Restringir el tiempo de conexión de los usuarios, considerando las necesidades de la Corporación.
e) Bloquear las cuentas de usuarios, cuando se ha sobrepasado los intentos de ingreso a la cuenta por error fallido de contraseña.
f) Desactivar a los usuarios que no han usado su cuenta por más de 3 meses.
g) Evitar que se desplieguen mensajes de ayuda durante el procedimiento de registro de inicio de sesión.
h) Llevar un proceso de monitoreo y registro de los intentos exitosos y fallidos de autenticación del sistema, registros de alarmas cuando se violan las políticas de seguridad del sistema.
i) Controlar que no se muestren identificadores de aplicación ni de sistema, hasta que el proceso de registro de inicio se haya completado exitosamente.

El área de Talento Humano deberá:

j) Dar aviso a la Mesa de Servicios sobre la salida de un Servidor a fin de proceder con la eliminación o desactivación de todas las cuentas que le hayan sido asignadas y en todos los servicios.

3. GESTIÓN DE USUARIOS

3.1. Identificación y autenticación de usuarios

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberán:

a) Rastrear utilizando los identificadores de usuario y evidenciar las actividades de las personas responsables de administraciones críticas de la Corporación.
b) Velar por que las actividades de usuarios regulares no sean realizadas desde cuentas privilegiadas.
c) Utilizar métodos alternos a la contraseña, como los medios criptográficos, las tarjetas inteligentes, tokens o medios biométricos de autenticación, cuando fuera posible.

d) El registro de usuarios debe realizarse primero en el directorio activo de la Corporación y luego en cualquiera de los sistemas o servicios que el funcionario requiera.
e) Los sistemas existentes en la Corporación deben autenticar a los usuarios usando el Directorio Activo de la Corporación, siempre y cuando sea tecnológicamente posible.

3.2. Creación de usuarios

a) Previo a la creación de un usuario, el Servidor responsable del mismo debe firmar el compromiso de confidencialidad conforme a la "Guía de contratos y compromiso de confidencialidad".

Para la creación de usuarios, el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberán:

b) Usar como excepción, y solo por temas de necesidad de la Corporación, identificadores de usuarios para un grupo de usuarios o de trabajo específico, el cual debe estar definido y documentado.
c) Los usuarios serán creados a partir de una solicitud de las áreas de Talento Humano a la Mesa de Servicios, previa la autorización de la Subdirección o Jefaturas de Tecnologías de Información y Comunicaciones de la Corporación y será activado posterior a la firma del Compromiso de Confidencialidad.
d) Para la creación de usuarios se debe enviar la siguiente información:
¡Error! Vínculo no válido.
e) Evitar el uso de usuarios genéricos. De preferencia, se deberá usar la opción "enviar como" del servicio de Correo Electrónico, para lo cual se deberá enviar una solicitud a la Mesa de Ayuda para su configuración.
Cuando se requiera la creación de este tipo de usuarios, se enviará una solicitud a la Subdirección de Tecnologías de Información de Matriz de manera formal, firmada por el Gerente de la Unidad de Negocio o el Director de Gestión Estratégica en el caso de Matriz, adjuntando:
    - Compromiso de Confidencialidad suscrito por el Servidor que será responsable del manejo de la cuenta
    - Justificación bien sustentada sobre la necesidad
    - Formulario de creación de cuentas debidamente lleno
f) Los nuevos usuarios en todos los sistemas, nombrarán de la siguiente manera, en orden de prioridad de acuerdo a la existencia o no de coincidencias:
    - primernombre.primerapellido

- segundonombre.primerapellido
- De persistir coincidencias, se hará uso de la primera letra del segundo nombre y/o apellido.
- Se dará prioridad de la siguiente manera:
    i. De acuerdo al tiempo que trabajan en la corporación.
    ii. De acuerdo al cargo que desempeñen dentro de la corporación.
    iii. La primera vez se crearán todos los usuarios en estricto orden alfabético.

g) Para las cuentas genéricas se tomará como “primernombre” el área o función de la cuenta y como “primerapellido” las siglas de la unidad de negocio interesada que constan en el sistema IFS.

3.3. Registro de usuarios

El Operador de seguridad en conjunto con el área de TIC y/o los Administradores de Sistemas de Operación y Control deberán:

a) Establecer un procedimiento formal, documentado y difundido, en la administración de los perfiles y roles de las cuentas de los usuarios. en el cual se evidencie detalladamente los pasos y responsables para:
    - Definir el administrador de accesos que debe controlar los perfiles y roles;
    - Gestionar el documento de requerimiento de accesos de los usuarios tanto internos como externos, que contemple: el solicitante del requerimiento o iniciador del proceso, validación del requerimiento, autorizador del requerimiento, ejecutor del requerimiento, forma y medio de entrega del acceso al usuario (manteniendo confidencialidad);
    - Crear los accesos para los usuarios.
    - Modificar los accesos de los usuarios;
    - Eliminar los accesos de los usuarios;
    - Suspender temporalmente los accesos de los usuarios en caso de vacaciones, comisiones, licencias, es decir, permisos temporales;
    - Proporcionar accesos temporales a usuarios externos o terceros de acuerdo al tiempo de su permanencia y limitados según las actividades para las que fueron contratados y firmar un convenio de confidencialidad;
    - Mantener un registro de la gestión de accesos a aplicaciones, redes, que evidencie, fecha de creación, eliminación,

suspensión, activación o eliminación del acceso; al igual que de cada usuario, disponer de los permisos de acceso que han sido asignados.

3.4. Identificación y autenticación de usuarios

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberán:

a) Usar como excepción, y solo por temas de necesidad de la Corporación, identificadores de usuarios para un grupo de usuarios o de trabajo específico, el cual debe estar definido y documentado.
b) Velar por que las actividades de usuarios regulares no deben ser realizadas desde cuentas privilegiadas.
c) Garantizar que la identificación de usuario es única e intransferible, por lo que, debe estar registrado y evidenciado en la política de accesos que no se permite el uso de una identificación de usuario de otra persona.
d) Permitir un máximo de tres intentos de registro de inicio de sesión a los sistemas y habilitar un tiempo de dilación antes de permitir o rechazar más intentos adicionales del registro de inicio sin autorización específica.
e) Validar la información de registro de inicio únicamente cuando el usuario termine de ingresar todos los datos de entrada, y en el caso que se presentara un error o se generara sentencias de error, el sistema no indique qué parte de los datos es correcta o incorrecta o emita mensajes propios de las características del sistema.

3.5. Administración de Privilegios

El Operador de seguridad en conjunto con el área de TIC y/o el Administrador de sistemas de Operación y Control deberá:

a) Controlar la asignación de privilegios a través de un proceso formal de autorización.
b) Mantener un cuadro de identificación de los usuarios y sus privilegios asociados con cada servicio o sistema operativo, sistema de gestión de base de datos y aplicaciones.
c) Evidenciar documentadamente que cada activo de información tecnológico tenga definido los niveles de acceso basados en perfiles y

permisos, a fin de determinar que privilegios se deben asignar según las actividades de los usuarios y la necesidad de la Corporación y su función.

3.6. Cuentas Usuarios Administradores

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberán:

a) Bloquear o eliminar usuarios “por defecto” según el sistema o fabricante del producto.
b) Cambiar las contraseñas de sistemas (cuentas de administración de aplicaciones, cuentas de administrador, entre otras) al menos cada 6 meses.
c) Cambiar las contraseñas “por defecto” asociadas a los sistemas o aplicaciones antes de ponerlas en producción.

3.7. Autenticación de usuarios para conexiones externas

El Operador de seguridad en conjunto con el área de TIC y/o el Administrador de sistemas de Operación y Control deberá:

a) Realizar un mecanismo diferenciado para la autenticación de los usuarios que requieren conexiones remotas, que permita llevar control de registros (logs) y que tenga limitaciones de accesos en los segmentos de red.

4. GESTIÓN DE CONTRASEÑAS

La asignación de contraseñas se controlará a través de un proceso formal de gestión a cargo del Área de TIC. Las acciones establecidas en este punto estarán a cargo del área de TIC o del Servidor según corresponda.

4.1. Seguridad de las contraseñas

a) Las contraseñas son personales e intransferibles, siendo el dueño de la cuenta responsable de lo que se realice a través de su cuenta, con

y sin su conocimiento.

b) Las claves que son enviadas por parte de los administradores, deben cumplir con las características establecidas en esta Guía. Posterior a su envío, se debe habilitar la opción para obligar al usuario a cambiarla.
c) Las contraseñas “por defecto” de los sistemas, aplicaciones y/o equipo deben ser cambiadas en el primer inicio de sesión.
d) Las contraseñas deben cumplir con las características mínimas establecidas en la presente Guía.
e) Las claves en blanco deben ser cambiadas y se debe desactivar la opción de dejar una clave en blanco, en todo servicio o sistema.
f) Las contraseñas son manejadas como información confidencial. Es responsabilidad del usuario todas las acciones que se realicen con ellas.
g) Se realizará una auditoría de contraseñas 2 veces al año, tanto de usuario como de aplicaciones o servicios.

4.2. Duración de las contraseñas

a) Todos los Servidores deberán cambiar sus claves o contraseñas, cada días para toda cuenta personal o genérica que haya sido otorgada por la Corporación.
b) El área de TIC y/o los Administradores de Sistemas de Centros de Operación y Control deberán adecuar los sistemas para que soliciten el cambio obligatoriamente transcurrido los 180 días.
c) Los Servidores no deben repetir las 2 anteriores claves o contraseñas utilizadas en el servicio o sistema, el área de TIC y/o los Administradores de Sistemas de Centros de Operación y Control deberán adecuar los sistemas para que hagan este control.

4.3. Restricciones de las contraseñas

a) Los Servidores no deben revelar contraseñas de manera directa, por teléfono o respuesta a mensajes de correo electrónico.
b) Los Servidores no deben almacenar las contraseñas en programas gratuitos o pagados que tengan esta facilidad.
c) Las contraseñas no deben estar a disposición de terceros, de manera legible en medios impresos o físico, en caso de ser necesario su registro debe ser un lugar seguro y controlado.
d) Las contraseñas de cuentas personales no deben ser la misma que

para cuentas genéricas.

4.4. Estándar para contraseñas

Todos los Servidores deberán seguir el siguiente estándar para la generación de contraseñas, de la misma manera, los sistemas deberán estar configurados para controlar que las contraseñas lo cumplan:

a) Las contraseñas deben tener al menos ocho caracteres
b) Las contraseñas deben incluir:
    - Combinación de mayúsculas, minúsculas (desde A/a a la Z/z no Ñ/ñ).
    - Números (desde el 0 al 9)
    - Opcionalmente debe incluir caracteres no alfanuméricos (como #,",@,%,$,&,/).
    - No debe repetirse por lo menos 2 contraseñas anteriores en el mismo sistema o servicio.
    - La longitud mínima de la contraseña será de 8 caracteres.
c) No deben incluir nombres o apellidos del usuario, más de tres caracteres consecutivos.

4.5. Bloqueo de contraseñas

a) En los casos en que se desactive el acceso, el administrador del servicio o sistema debe asignar una clave temporal al usuario.
b) Las claves temporales deben ser cambiadas por el usuario en el ingreso al sistema inmediatamente posterior a la configuración de la clave mencionada.
c) El área de TIC y/o los Administradores de Sistemas de Centros de Operación y Control deberán adecuar los sistemas para que las cuentas se bloqueen cuando:
    - Se introduce más de 3 veces seguidas la contraseña errónea. En este caso el bloqueo será temporal por 10 minutos, luego de lo cual será desbloqueada automáticamente. Este tipo de bloqueos puede repetirse solamente 2 veces seguidas, después de lo cual la cuenta quedará bloqueada hasta que se dirija una solicitud de desbloqueo al administrador.
    - Las cuentas registren inactividad por 30 días sin aviso previo

justificado. El bloqueo tendrá validez hasta que se dirija una solicitud de desbloqueo al administrador.

- Un Servidor sale de la empresa, en cuyo caso el bloqueo será permanente.

4.6. Documentación para la Gestión de Contraseñas

En las áreas de TIC, el Operador de Seguridad de Información constatará que exista la siguiente documentación para la gestión de contraseñas:

a) Inventario de usuarios creados, en el caso de cuentas genéricas identificar su responsable.

Nro.	Usuario	Responsable	Fecha de Creación	Tipo	Fecha de eliminación o bloqueo	Permisos asignados
				Fijo/Temporal		

b) Procedimiento para cambio de contraseñas de nuevos usuarios y usuarios existentes.
c) Sección de cambio de contraseñas en los Manuales de Usuario..
d) Catálogo de servicios con la asignación de responsables, identificando tiempos de respuesta para la creación de usuarios, desbloqueo de contraseñas y cambio de contraseñas.

5. USO ADECUADO DE ESTACIONES DE TRABAJO

El área de TIC deberá:

a) Implementar medidas para que, en un determinado tiempo (ej., no mayor a 10 minutos), si el usuario no está realizando ningún trabajo en el equipo, se bloquee su sesión automáticamente. El desbloqueo se dará únicamente si el usuario ingresa nuevamente su clave.
b) Bloquear las copiadoras y disponer de un control de acceso especial para horario fuera de oficinas.
c) Retirar información sensible una vez que ha sido impresa.
d) Retirar información sensible, como las claves, de sus escritorios y pantallas.

e) Retirar los dispositivos removibles una vez que se hayan dejado de utilizar.

5.1. Puesto de trabajo despejado y pantalla limpia

El Operador de Seguridad en conjunto con el área de TIC deberá:

a) Desconectar de la red, servicio o sistema, las computadoras personales, terminales, impresoras asignadas a funciones críticas, cuando se encuentren desatendidas. Por ejemplo, haciendo uso de protectores de pantalla con clave.
b) Proteger los puntos de recepción de correo postal y fax cuando se encuentren desatendidas.
c) Cifrar los discos duros de los computadores personales (escritorio, portátiles, etc.) y otros dispositivos que se considere necesarios, de las máximas autoridades de la Corporación.

El Oficial de Seguridad de la Información deberá gestionar:

d) Actividades periódicas (una vez cada mes como mínimo) para la revisión al contenido de las pantallas de los equipos, con el fin de que no se encuentren iconos y accesos innecesarios, y carpetas y archivos que deben ubicarse en la carpeta de documentos del usuario.
e) Mantener bajo llave la información sensible (cajas fuertes o gabinetes), en especial cuando no estén en uso y no se encuentre personal en la oficina.

5.2. Procedimiento de registro de inicio seguro

El área de TIC deberá:

a) Autenticar usuarios autorizados, de acuerdo a la política de control de acceso de la Corporación, que deberá estar documentada, definida y socializada.
b) Llevar un registro de definición para el uso de privilegios especiales del sistema.
c) Llevar un proceso de monitoreo y registro de los intentos exitosos y fallidos de autenticación del sistema, registros de alarmas cuando se violan las políticas de seguridad del sistema.
d) Utilizar mecanismos como: uso de dominios de autenticación,

servidores de control de acceso y directorios.

e) Restringir el tiempo de conexión de los usuarios, considerando las necesidades de la Corporación.
f) Controlar que no se muestren identificadores de aplicación ni de sistema, hasta que el proceso de registro de inicio se haya completado exitosamente.
g) Evitar que se desplieguen mensajes de ayuda durante el procedimiento de registro de inicio de sesión.
h) Validar la información de registro sin emitir mensajes propios de las características del sistema.
i) Limitar la cantidad de intentos permitidos de registro de inicio de sesión; por ejemplo, tres intentos.
j) Limitar el tiempo de dilación antes de permitir o rechazar más intentos adicionales del registro de inicio sin autorización específica.

5.3. Identificación de los equipos en las redes

El área de TIC deberá:

a) Identificar y documentar los equipos que se encuentran en las redes.
b) Tener documentada la identificación de los equipos que están permitidos, según la red que le corresponda.
c) Utilizar métodos para que la identificación del equipo esté en relación a la autenticación del usuario.

5.4. Protección de los puertos de configuración y diagnóstico remoto

El Operador de seguridad en conjunto con el área de TIC deberá:

a) Establecer un procedimiento de soporte, en el cual se garantice que los puertos de diagnóstico y configuración sean sólo accesibles mediante un acuerdo entre el administrador del servicio de computador y el personal de soporte de hardware/ software que requiere el acceso.
b) Los puertos, servicios (ej., ftp) que no se requieren por necesidades de la Corporación, deberán ser eliminados o deshabilitados.

5.5. Control de conexión a las redes

El Operador de seguridad en conjunto con el área de TIC deberá:

a) Aplicar filtros a la conexión de los usuarios, a través de puertas de enlace de red (gateway) que controlen el tráfico por medio de tablas o reglas predefinidas, conforme a los requerimientos de la Corporación.
b) Aplicar filtros considerando, entre otras cosas:
    - Mensajería
    - Transferencia de archivos
    - Acceso interactivo
    - Acceso a las aplicaciones
    - Horas del día y fechas de mayor carga
c) Incorporar controles para restringir la capacidad de conexión de los usuarios a redes compartidas especialmente de los usuarios externos a la Corporación.

5.6. Trabajo remoto

a) Todos los Servidores procurarán evitar la conexión a redes inalámbricas que no presten la seguridad de acceso y autenticación adecuados.
b) El jefe inmediato deberá definir los sistemas y servicios internos para los cuales el Servidor tiene acceso autorizado y enviar esta información al área de TIC, así como el trabajo que se permite realizar y el horario.
c) El área de TIC deberá implementar la protección por antivirus y reglas del Firewall.
d) La Corporación deberá observar la disposición de una póliza de seguros para esos equipos, a través del área de Abastecimientos o Seguros según corresponda.
e) El Operador de Seguridad deberá determinar procesos de monitoreo y auditoría de la seguridad del trabajo remoto que se realice.

5.7. Computación y comunicaciones móviles

El Operador de Seguridad de Información en conjunto con el área de TIC deberá:

a) Definir rangos de tiempo máximo que el equipo puede permanecer sin conexión a la red de la Corporación, después del cual se deberá emitir alertas por no actualización de antivirus y la no aplicación de las políticas de los sistemas Corporativos.
b) Considerar principalmente, en el proceso de respaldo del equipos, los documentos definidos como críticos, sensibles o confidenciales.
c) Proveer reglas para asegurar los equipos portátiles de la Corporación así como los medios físicos,

6. USO ADECUADO DEL CORREO ELECTRÓNICO

6.1. Responsabilidad por el uso del correo electrónico

a) El Servidor es el único responsable por todas las actividades realizadas con la cuenta de correo electrónico proporcionado por la Corporación.
b) El Servidor debe velar por el buen uso de los recursos que integran dicha cuenta y particularmente, los elementos, como la clave de usuario, que pueden permitir el acceso no autorizado a terceras personas a todos los recursos tecnológicos asignados.

6.2. Mantenimiento de buzón

a) El Servidor debe continuamente eliminar aquellos mensajes que entienda como no importantes para la empresa, evitando así la saturación del espacio asignado a su buzón de correo electrónico.
b) El Servidor debe guardar todos los documentos que considere importantes para la Corporación en su unidad local.

6.3. Uso de correo electrónico

a) La cuenta de correo electrónico asignada a los Servidores de la Corporación, debe ser usada exclusivamente para actividades de la misma, no obstante estarán disponibles el acceso a servicios gratuitos para fines personales (Hotmail, Yahoo, Gmail, etc.).
b) Si el Servidor detecta que su cuenta está siendo utilizada por una tercera persona, debe cambiar su clave de usuario y notificar inmediatamente lo ocurrido, conforme a la “Guía de gestión de

incidentes de seguridad de información".

6.4. Prohibiciones al uso de correo electrónico

Para efectos de un mejor servicio, está prohibido:

a) El uso de mecanismos y sistemas que intenten ocultar la identidad del emisor de correo.
b) La suplantación de identidad de otra persona en el envío de mensajes de correo electrónico.
c) El uso de los sistemas de comunicación electrónica de CELEC EP para actividades de proselitismo político o religioso, así como cualquier actividad que pueda de alguna manera afectar la honra, el buen nombre de una persona o la moral y las buenas costumbres.
d) El uso del buzón de correo electrónico como repositorio de almacenamiento de información distinta a la enviada o recibida por este medio y con fines distintos a los establecidos en esta Guía.
e) El envío de correo electrónico a personas que no desean recibirlo (SPAM).
f) La propagación de "cartas en cadena" o esquemas piramidales de cualquier índole.
g) El uso del correo electrónico con información que atente a la integridad, imagen y reputación de la empresa o de sus colaboradores.

El incumplimiento a esta disposición es considerada una falta leve y será sancionada de acuerdo a lo previsto en el Art. 50.1 del Reglamento Interno de Trabajo de la Corporación, a excepción de la suplantación de identidad que es considerada una falta grave y será sancionada de acuerdo a lo establecido en el Art. 50.2 del Reglamento Interno de Trabajo de la Corporación.

6.5. Recepción de correo electrónico de origen desconocido

a) El usuario no debe abrir o ejecutar archivos adjuntos de correos dudosos ya que podrían contener códigos maliciosos (virus, troyanos, gusanos, etc.).
b) Si recibe mensajes de este tipo, el usuario debe comunicarlo de manera inmediata conforme a la "Guía de gestión de incidentes de seguridad de información".

6.6. Elaboración de correo electrónico

a) Todo lo que se envíe bajo el dominio de la Corporación puede entenderse remitido en representación de la misma. Teniendo esto en cuenta, los contenidos de los correo enviados serán de exclusiva responsabilidad del usuario de la cuenta. Por ello antes de enviar el mensaje, el Servidor deberá revisar cuidadosamente el contenido del correo y corregirlo de ser necesario, evitando cualquier forma de vulgaridad, discriminación, ilegalidad, etc.

6.7. Servicio de directorio activo

a) El Servicio de Directorio Activo es el centro de seguridad y control de acceso donde reside la información de cuentas y clave de usuarios. El Servidor debe asegurarse que su información de contacto, como extensión telefónica, cargo, lugar de trabajo y otros, se mantengan actualizados.
b) En caso de haber cambios en los mismos o diferencias, el Servidor debe enviar una notificación a la Subgerencia Administrativa correspondiente o a la Dirección Administrativa Financiera de Matriz quien a su vez lo comunicará mediante correo electrónico a la Mesa de Servicios.

6.8. Servicio de Correo electrónico

a) Dado que actualmente el servicio de correo electrónico se usa intensivamente, el Servidor es responsable del buen uso del mismo, y debe evitar el envío de correo electrónico no deseado.
b) El Servidor debe mantener los límites de almacenamiento definidos por la Corporación para su buzón de correo electrónico.
c) El Servidor debe respetar los límites de envío y recepción de mensajes definidos en la Corporación y procurar el revisar su buzón de correo electrónico por lo menos una vez al día, considerando de que el no haber leído un mensaje que se encuentra en su bandeja es su responsabilidad. La cantidad de archivos adjuntos no deberá superar el máximo establecido para tal efecto que asciende a 20MB.

6.9. Acceso al buzón de correo electrónico de otro usuario

a) Esta prohibido que un usuario entre al buzón de correo de otro usuario. Únicamente con autorización del Gerente General, Gerente de unidad de negocio, Directores de Matriz o del titular de la cuenta a través de un correo a la Mesa de Servicios, el área de TIC puede entregar el acceso o una copia del buzón de un funcionario.

GLOSARIO DE TÉRMINOS

- **Bloqueo Cuenta:** Suspender temporalmente los accesos a un sistema de información, por novedades como: vacaciones, licencias, incapacidades del funcionario.
- **Cuentas de Usuarios:** cuentas personales que dan acceso a servicios o sistemas informáticos corporativos como cuentas de correo, cuentas de acceso a la red entre otros.
- **Cuentas de Administradores:** cuentas personales que dan acceso a sistemas o recursos informáticos con privilegios y permisos de administración, como cuentas a equipos de comunicación, cuentas de administración de sistemas operativos, cuentas de administración de aplicaciones o sistemas.
- **Cuentas Genéricas:** cuentas que tienen un responsable asignado para su administración, pueden ser utilizadas para grupos de trabajo como en correo electrónico, o usuarios de pruebas en sistemas y aplicaciones.
- **Crear Cuenta:** Asignar una identificación (usuario y una contraseña) para acceder a un sistema de información; por ejemplo equipo, programas, entre otros.
- **Desactivar Cuenta:** Aplica para casos como retiro definitivo, traslados, o fallece un funcionario.
- **Desbloqueo Cuenta:** Liberar los servicios de acceso a un sistema de información o equipo.
- **Eliminar Cuenta:** Aplica para el Correo Electrónico; no se pueden recuperar los emails, una vez borrada la cuenta.

Sección IV

Guía de contratos y compromisos de confidencialidad

SIC-GLG-001-2014

Revisión 2

Diciembre - 2014

CONTENIDO

INTRODUCCIÓN

A fin de garantizar la confidencialidad, disponibilidad e integridad de la información en la Corporación, es necesario implementar una Guía de Contratos y Compromiso de Confidencialidad, que permitan controlar la gestión de la información en la Corporación, teniendo en consideración que toda la información generada pertenece a la Corporación, y en tal sentido es responsabilidad de los Servidores dar un buen uso a la administración de la misma.

La información que genere el Servidor, tal como programas, aplicaciones, planos, diagramas, cálculos u otros instrumentos que permitan mejorar procesos internos y automatización de tareas, son propiedad de la Corporación, de acuerdo al Art 45. del Reglamento Interno de Trabajo de CELEC EP.

ALCANCE

- La guía pretende establecer las responsabilidades de los Servidores y el buen uso responsable de la información en la Corporación.
- Establecer un Compromiso de Confidencialidad, a través del cual se determinen las obligaciones del Servidor respecto al buen uso de la información en la Corporación.

OBJETIVO

- Responsabilizar y concientizar al Servidor, el buen uso de la información.
- Establecer, oficializar y difundir el Compromiso de Confidencialidad.
- Establecer procedimientos que permitan garantizar la integridad, disponibilidad y confidencialidad de la información, al inicio, durante y al finalizar la relación laboral entre el Servidor y CELEC EP.

1 OBLIGACIONES DEL SERVIDOR

El Reglamento Interno de Trabajo de CELEC EP Capítulo VI, Título III de las Obligaciones de los Servidores Art. 44.9, establece: “Guardar estricta reserva y confidencialidad sobre la información de la Corporación que le sea entregada, la que genere como consecuencia de sus actividades y en general la que llegue a conocer por el desempeño de su puesto de trabajo, incluyendo la información que conste en medio de audios y videos ya sea físicos o magnéticos y en cualquier formato que permita el almacenamiento de datos”.

Para todos los activos de información, y los puntos señalados en esta Guía, en las Normas, Instructivos, Procedimientos y Reglamentos de la Corporación se deberá considerar que el grado de confidencialidad con el que se deberá tratar a los activos de información de la Corporación dependerá de la clasificación de los mismos y de los permisos que el Propietario otorgue sobre ellos a los responsables, de conformidad con la “Guía de Gestión de Activos de Información”.

El Servidor deberá cumplir con todos los procedimientos establecidos por CELEC EP durante y al finalizar su relación de dependencia laboral con la Corporación.

1.1 Ingreso a la Corporación

De acuerdo a lo establecido en la Norma Técnica de Seguridad de Información de la Corporación, es menester de las Áreas de TIC, mantener la información de la Corporación íntegra, disponible y confiable. El Servidor que ingresa a la Corporación deberá cumplir con lo siguiente:

f) Suscribir un acta entrega-recepción de equipos informáticos, emitida por el Área de Control de Bienes, con copia al Área de TIC.
g) Suscribir un formulario que contenga la lista de servicios informáticos y programas al que el Servidor tendrá acceso para su trabajo diario, emitida por parte del Responsable del Área en la cual labora el Servidor.
h) En el formulario del punto b) se harán constar los acuerdos de control de accesos que contemplen:
    - Permisos, perfiles y uso de identificadores únicos.
    - Autorización de accesos y privilegios de usuarios.
i) Administrar con responsabilidad los bienes a su cargo.

j) El Servidor no deberá utilizar usuarios diferentes a los asignados por la Corporación, para el uso de los servicios o sistemas.
k) Cambiar la contraseña temporal, inicialmente generada por el área de TIC para la cuenta de usuario a los servicios requeridos, previo formulario suscrito por el solicitante, de manera inmediata. Caso contrario el servicio se bloqueará al iniciar nuevamente la sesión y se deberá solicitar una nueva contraseña.
l) Cumplir con las Políticas, Normas Técnicas, Guías, Procedimientos e Instructivos de Seguridad de Información establecidas por la Corporación, las cuales serán puestas en conocimiento de los Servidores por parte del área de Talento Humano.
m) Mantener los niveles de confidencialidad, disponibilidad e integridad de los activos de información que tiene a su cargo, dando buen uso a los mismos.
n) Suscribir el Compromiso de Confidencialidad en el Área de Talento Humano, establecido por la Corporación, el mismo que deberá ser accesible al Oficial de Seguridad de Información. (Anexo A: Compromiso de Confidencialidad)

1.2 Traslados, cambios administrativos y separación de la corporación

En el caso de que un Servidor se traslade a dentro de otras Unidades de Negocio o hacia Matriz, se deberá proceder de la siguiente manera:

a) El área de Talento Humano notificará a las áreas correspondientes, el cambio de estado del Servidor, mediante formularios suscritos que evidencien este requerimiento.
b) El responsable de la administración de los activos de información del área de TIC, actualizará el estado de los mismos y se informará del particular al Equipo de Seguridad de Información, mediante formularios estandarizados, suscritos por el responsable de la administración de los activos de información.
c) El área de TIC eliminará los accesos a los servicios o efectuará los cambios que correspondan y realizará los respaldos de toda la información. El técnico responsable, deberá emitir un informe que evidencie esta actividad.
d) El delegado de TIC debe entregar el informe al Equipo de Seguridad sobre el estado de los activos de información.

e) El Servidor, debe entregar un informe de temas pendientes y las actividades que hasta el momento se encuentra realizando a su Jefe inmediato, de acuerdo al Art. 44.26 del Reglamento Interno de Trabajo, de la cual se dejará constancia escrita.

Además de lo establecido en los literales anteriores, cuando un Servidor termine su relación laboral con la Corporación, se deberá proceder de la siguiente manera:

f) El Servidor entregará los bienes a su cargo al área de Abastecimientos. El responsable de bodega y el delegado de TIC estarán presentes para realizar la verificación en sitio de la entrega y el estado de los mismos.
g) El Área de Talento Humano notificará el término de relación de dependencia de un Servidor al Equipo de Seguridad de Información.

2 RESPONSABILIDADES DEL SERVIDOR Y LA CORPORACIÓN

2.1 Responsabilidades del Servidor

a) La conservación, buen uso y mantenimiento de los bienes, será responsabilidad directa del Servidor que los ha recibido para el desempeño de sus funciones y labores oficiales.
b) En cumplimiento al "Reglamento Interno de Trabajo de CELEC EP", el Servidor deberá:
    - "Guardar estricta reserva y confidencialidad sobre la información de la Corporación que le sea entregada, la que genere como consecuencia de sus actividades y en general la que llegue a conocer por el desempeño de su puesto de trabajo, incluyendo la información que conste en medio de audios y videos ya sea físicos o magnéticos y en cualquier formato que permita el almacenamiento de datos. Por lo cual el Servidor deberá cumplir con los procedimientos establecidos por CELEC EP desde el ingreso hasta la finalización de su relación de dependencia con la Corporación". Los niveles de reserva y confidencialidad serán definidos aplicando la "Guía de Gestión de Activos de Información"
    - "Mantener en buenas condiciones los equipos, maquinarias y en general los implementos que la Corporación le entregue para la realización de sus actividades. En caso de existir algún

inconveniente se deberá informar al Jefe inmediato con copia al Área de Bienes y Área de TIC, quienes deberán disponer al Responsable de la administración de activos, ejecutar las acciones necesarias para restaurar el activo. Toda anomalía que atente contra la seguridad de la información de la Corporación, deberá ser notifica al Oficial de Seguridad de Información".

- "Administrar y salvaguardar la información que conozca y genere para la Corporación, absteniéndose de entregar a cualquier persona, salvo autorización o disposición expresa, copias u originales de documentos o información digital en los que conste, actas, diagramas, cálculos, planos u otros documentos de propiedad de la Corporación y cuya difusión o conocimiento por parte de terceros pueda entrañar perjuicio comercial o de otra índole. Tomando en consideración la confidencialidad y reserva de los datos de acuerdo al Art. 5 de la Ley de Comercio Electrónico." Los niveles de reserva y confidencialidad serán definidos aplicando la "Guía de Gestión de Activos de Información"

c) El Servidor, al finalizar su dependencia laboral con la Corporación, deberá entregar los bienes y activos de información que se encuentren a su cargo y, en cumplimiento del Art. 44.11 del Reglamento Interno de Trabajo, deberán haber sido mantenidos en buenas condiciones. De darse la desvinculación del Servidor, el área de Tecnologías de la Información analizará los bienes (equipos informáticos) asignados al Servidor para determinar si existen daños que se imputen al mal uso o si los mismos corresponden al desgaste normal en consideración al estado de los equipos. En caso de encontrarse desperfectos no justificados, se procederá como se establezca en la normativa existente para el efecto.

d) El Servidor será responsable de los activos de información que administre, por lo que, en caso de existir algún incidente como robo, suplantación, pérdida, fuga de información, entre otras, el Servidor será quien notifique estos incidentes al Jefe inmediato, con copia al Oficial de Seguridad de Información.

2.2 Responsabilidades de la Corporación

a) El administrador de los activos de información del área de TIC deberá presentar al Oficial de Seguridad Corporativo, para su aprobación, un cronograma anual en el que se detalle el período de verificación y revisión de los activos de información de la Corporación.

b) Para verificar el estado de los activos de información entregados, el administrador de los mismos emitirá un informe en el cual se

detallarán las anomalías encontradas y presentará al Jefe Inmediato del Servidor. El informe, de considerarse necesario, será puesto en conocimiento del Oficial de Seguridad.

c) El responsable de los activos de información del área de TIC, deberá aplicar controles apropiados para garantizar la integridad de los mismos una vez finalizada la relación de dependencia del Servidor con la Corporación, o en un momento convenido durante la vigencia del contrato.
d) El Área de Talento Humano deberá notificar, al área de TIC, la finalización de la relación de dependencia laboral entre el Servidor y la Corporación, a fin de desactivar todas las cuentas de usuarios del Servidor, realizar respaldos de toda la información y emitir informe de estados.
e) El Área de TIC establecerá, al inicio de cada año, un cronograma en el cual se detallen las fechas en las que se van a efectuar los respaldos de acuerdo a la criticidad de la información a ser respaldada. Este cronograma deberá ser comunicado al Oficial de Seguridad de Información.
f) De existir algún inconveniente con los activos de información y este daño atente con la integridad, disponibilidad y confidencialidad de la información, el administrador de los activos de información del Área de TIC notificará de este suceso al Oficial de Seguridad de Información.
g) La Corporación formalizará el Compromiso de Confidencialidad para todos sus Servidores.
h) Los Compromisos de Confidencialidad, serán suscritos previa contratación de un nuevo Servidor: En el archivo personal de cada Servidor, se mantendrá el original del Compromiso y una copia del mismo será remitida por parte del Área de Talento Humano al Oficial de Seguridad de Información, en caso de ser requerido.
i) La Corporación, a través del Equipo de Seguridad de Información, podrá verificar el cumplimiento de lo establecido en el Compromiso de confidencialidad.

3 COMPROMISO DE CONFIDENCIALIDAD CON TERCEROS

a) En el marco de los contratos o convenios suscritos por CELEC EP, dentro de los cuales se genere información de forma conjunta entre los Servidores de la Empresa y los Contratista, y si a criterio de CELEC EP es necesario, se podrá efectuar compromisos de confidencialidad, con la finalidad de garantizar la confidencialidad de

la información que sea manejada internamente por parte de Servidores de CELEC EP y por parte de terceros para la ejecución del contrato, los mismos que serán avalados por el administrador el contrato o convenio. Para cumplir con este requisito, se usará el formato de “Compromiso de confidencialidad con terceros” Anexo B de esta Guía.

b) El Administrador del contrato o convenio entregará una copia del documento en el cual se refleje la Cláusula de Confidencialidad, al Oficial de Seguridad de Información para su monitoreo, control y cumplimiento.

c) El administrador de Servidores, equipos de comunicaciones o de seguridad, deberá realizar un cronograma de monitoreo de dichos activos, previo análisis de acuerdo a la importancia del activo. Este cronograma se deberá acordar con los terceros que por motivo de mantenimiento o soporte tengan acceso remoto a los activos mencionados en este punto.

ANEXO A: COMPROMISO DE CONFIDENCIALIDAD

_____ en adelante "Servidor", con cédula de ciudadanía número _____, en virtud de la relación laboral bajo dependencia que mantiene con la Empresa Pública Estratégica Corporación Eléctrica del Ecuador CELEC EP, en adelante "Corporación", desde el _____, con relación a la utilización de la "Clave de Usuario", "Tecnología" y "Activos de Información", para el cumplimiento de sus actividades y otros deberes formales, así como uso de los sistemas de información y acceso a otros servicios que la "Corporación" ponga a su disposición a través de Internet o de la Red interna; declara expresamente que conoce, acepta y se compromete a:

El Servidor a través de la suscripción del presente se compromete a hacer uso de los sistemas de información y de los activos de información de la Corporación, para lo cual expresa su voluntad de recibir los usuarios y claves necesarios para su acceso, así como también la administración responsable de todo tipo de información que genere por las actividades diarias de trabajo, en conocimiento de que esta es propiedad de CELEC EP y como Servidor público es menester conservar y dar buen uso de la información.

Definiciones:

La notificación electrónica realizada a través del servicio de correo electrónico de la Corporación, implica el acto por el cual la Corporación da a conocer al Colaborador que ha sido registrado o dado de alta en uno de los sistemas.

A través de los sistemas informáticos de la Corporación, el Colaborador hará uso de mensajes de datos. Dichos mensajes de datos se los entiende como toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio.

Los documentos desmaterializados[6] en mensajes de datos, que contengan las firmas electrónicas correspondientes debidamente certificadas ante una de las entidades autorizadas serán considerados como información original.

Se reconoce la validez jurídica a la información que figure en los mensajes de datos de conformidad a lo establecido en el Art. 3 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

6 Art. 7.- Información original.- (…) Los documentos desmaterializados deberán contener las firmas electrónicas correspondientes debidamente certificadas ante una de las entidades autorizadas según lo dispuesto en el artículo 29 de la presente ley, y deberán ser conservados conforme a lo establecido en el artículo siguiente.

De acuerdo con los preceptos de este Compromiso, la información y los recursos que permiten su procesamiento, almacenamiento, administración y seguridad, son un activo de la Corporación que se debe proteger su integridad, disponibilidad y confidencialidad

Compromiso del Servidor

- El Servidor asume la responsabilidad total del uso del nombre de usuario y su clave, así como de la veracidad y calidad de la información en el cumplimiento de sus funciones o encargos de su competencia y la utilización de los activos de información que la Corporación ponga a su disposición.

- El Servidor deberá conservar y dar un buen uso y mantenimiento de los activos de información que le han sido entregados. Será su responsabilidad directa usarlos para el desempeño de sus funciones y labores oficiales.

- El Servidor será responsable de los activos de información que administre por lo que, en caso de existir algún incidente como robo, suplantación, pérdida, fuga de información, entre otras, el Servidor será quien notifique estos incidentes a de acuerdo a la Guía de Gestión de Incidentes de Seguridad de Información.

- Todas las transacciones informáticas realizadas a través de los sistemas de información de la Corporación se garantizarán mediante el usuario y la clave del Servidor; consecuentemente, de su uso se derivará todas las responsabilidades de carácter administrativo, civil y penal a las que haya lugar.

- El Servidor conoce y acepta que la Corporación puede revisar cualquier información que el Servidor haya generado y tener acceso a cualquier activo de información que se le haya asignado, levantando explícitamente el sigilo del activo de información hacia la Corporación para análisis relacionados con la Seguridad de Información. Está consciente que se harán auditorías periódicas del manejo de su usuario y clave.

- El Servidor conoce y acepta que la clave o claves asociadas a su nombre de usuario que sean utilizadas en sistemas de información de propiedad de la Corporación surtirán los mismos efectos que el de las firmas electrónicas establecidas en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, por lo que, tanto su funcionamiento como su aplicación se entenderán como una completa equivalencia funcional, técnica y jurídica. [7]

- El Servidor, de acuerdo a su nombre de usuario y clave asignados por la Corporación, accederá a los activos de información en los que se le otorgó permiso.

El Servidor se compromete también a:

---

[7] De conformidad con el "Convenio para uso de servicios electrónicos" de la Contraloría General del Estado y la "Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos"

- Informarse, entender, apoyar y cumplir con las Políticas, Normas, Guías, Procedimientos e Instructivos de Seguridad de Información y Tecnología de la Información Corporativas que gobiernan la protección, el uso y la operación de los activos de la información de la Corporación.
- Hacer buen uso de los activos de información de la Corporación a los cuales tiene acceso para propósitos de cumplir con las tareas de trabajo a él asignadas.
- Comprender que el usuario que le asignen y clave, para el acceso a cualquier sistema de información de la Corporación, son exclusivamente para su uso y para propósitos de su trabajo. Estar consciente que cualquier actividad en los sistemas, registrados con su usuario son de su responsabilidad, asumiendo en consecuencia todos los efectos que su uso cause.
- Entender que la clave (contraseña) es un mecanismo importante para la protección de los sistemas y aplicaciones. Entender además, que su manejo es personal e intransferible y acuerda no divulgar la(s) clave(s) de acceso a él asignadas a ninguna persona, bajo ningún concepto.
- Garantizar la confidencialidad, disponibilidad e integridad de la información que gestiona.
- La suscripción del presente instrumento implicará la aceptación de todas y cada una de las disposiciones aplicables establecidas en la Norma Técnica de Seguridad de Información, sus Guías, Procedimientos e Instructivos.

Restricción de responsabilidad de la Corporación

La Corporación no tiene responsabilidad por la exactitud, veracidad, contenido o por cualquier error en la información proporcionada por el Servidor, sea que se trate de errores humanos

Declaración

El Servidor conoce y acepta que la información que se procese, almacene, comunique, etc. a través de su dirección de correo electrónico asignada _____; y las acciones que se generen mediante o en los sistemas informáticos de la Corporación, a través de su nombre de usuario y contraseña asociados, son de su estricta responsabilidad.

El Servidor acepta que el usuario y clave que se le proporciona, la información que use, cree o edite, haciendo uso de los sistemas o medios electrónicos que se ponga a su disposición, son de propiedad de la Corporación, de conformidad con el Reglamento Interno de Trabajo vigente.

Duración

Este Compromiso de confidencialidad tendrá una duración indefinida a partir de la fecha de su suscripción por parte del Servidor, salvo para los activos de información perdieran el carácter de confidencial por haber sido revelados oficialmente al público por la CELEC EP.

Aceptación

Libre y voluntariamente, el Servidor declara su aceptación a todo lo establecido en el presente instrumento, sometiéndose a sus estipulaciones, y comprometiéndose a su estricto cumplimiento.

Fecha (dd/mm/aaaa): _____ / _____ / _____

f) _____

Servidor: _____

No. Cédula Identidad: _____

Cargo: _____

Unidad de Negocio: _____

ANEXO B: COMPROMISO DE CONFIDENCIALIDAD DE TERCEROS

(REPRESENTANTE LEGAL DEL TERCERO), con cédula de ciudadanía número _____, en mi calidad de _____ de la Compañía _____, en adelante "Contratista", que mantiene un contrato con la Empresa Pública Estratégica Corporación Eléctrica del Ecuador CELEC EP, en adelante "Corporación", desde el _____(DD/MM/AAAA), cuyo objeto es _____ _____ _____, para el cumplimiento de las actividades y otros deberes formales de la Contratista, el uso de los sistemas de información y acceso a los servicios que la "Corporación" ponga a nuestra disposición a través de Internet o de la Red interna; declara expresamente que conoce, acepta y se compromete a:

El Contratista, a través de la suscripción del presente se compromete en hacer uso de los sistemas de información y de los activos de información de la Corporación, que el Administrador de Contrato determine necesario para el cumplimiento de sus obligaciones contractuales, para lo cual expresa su voluntad de recibir los usuarios y claves necesarios para su acceso, así como también la administración responsable de todo tipo de información que genere por las actividades diarias de trabajo, en conocimiento de que esta es propiedad de CELEC EP.

Definiciones:

La notificación electrónica realizada a través del servicio de correo electrónico de la Corporación, o por Comunicación escrita física (Oficio), implica el acto por el cual la Corporación da a conocer al Contratista que ha sido registrado o dado de alta en uno de los sistemas.

A través de los sistemas informáticos de la Corporación, el Contratista hará uso de mensajes de datos. Dichos mensajes de datos se los entiende como toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio.

Los documentos desmaterializados[8] en mensajes de datos, que contengan las firmas electrónicas correspondientes debidamente certificadas ante una de las entidades autorizadas serán considerados como información original.

[8] Art. 7.- Información original.- (…) Los documentos desmaterializados deberán contener las firmas electrónicas correspondientes debidamente certificadas ante una de las

Se reconoce la validez jurídica a la información que figure en los mensajes de datos de conformidad a lo establecido en el Art. 3 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

De acuerdo con los preceptos de este Compromiso, la información y los recursos que permiten su procesamiento, almacenamiento, seguridad, administración y seguridad, son un activo de la Corporación que se debe proteger su integridad, disponibilidad y confidencialidad

Compromiso del Contratista

- El Contratista asume la responsabilidad total del uso del nombre de usuario y su clave, así como de la veracidad y calidad de la información en el cumplimiento de sus actividades, otros deberes formales y la utilización de los activos de información que la Corporación ponga a su disposición.

- El Contratista deberá conservar y dar un buen uso y mantenimiento de los activos de información que le han sido entregados (total o parcialmente), será su responsabilidad directa usarlos para el desempeño de sus actividades y deberes contractuales.

- Guardar estricta reserva y confidencialidad sobre la información de la Corporación que le sea entregada, la que genere como consecuencia de sus actividades y en general la que llegue a conocer por el cumplimiento del objeto del contrato, incluyendo la información que conste en medio de audios y videos ya sea físicos o magnéticos y en cualquier formato que permita el almacenamiento de datos.

- Administrar y salvaguardar la información que conozca y genere para la Corporación, absteniéndose de entregar a cualquier persona, salvo autorización o disposición expresa, copias u originales de documentos o información digital en los que conste, actas, diagramas, cálculos, planos u otros documentos de propiedad de la Corporación y cuya difusión o conocimiento por parte de terceros pueda entrañar perjuicio comercial o de otra índole.

- El Contratista será responsable de los activos de información que administre y co-responsable sobre los que actúe, por lo que, en caso de existir algún incidente como robo, suplantación, pérdida, fuga de información, entre otras, el Contratista será quien notifique estos incidentes al Administrador de Contrato, con copia al Oficial de Seguridad de Información.

---

entidades autorizadas según lo dispuesto en el artículo 29 de la presente ley, y deberán ser conservados conforme a lo establecido en el artículo siguiente.

Todas las transacciones informáticas realizadas a través de los sistemas de información de la Corporación se garantizarán mediante el uso de un usuario y la clave del Contratista, consecuentemente de ellas se derivará todas las responsabilidades de carácter administrativo, civil y penal a que haya lugar.

- El Contratista asume la responsabilidad total del uso del nombre de usuario y su clave, como titular de las mismas, debiendo cumplir con las obligaciones derivadas de tal titularidad.

- Conoce y acepta que la Corporación puede revisar cualquier información que el Contratista haya generado y tener acceso a cualquier activo de información que se le haya asignado, levantando explícitamente el sigilo del activo de información hacia la Corporación para análisis relacionados con la Seguridad de Información. Está consciente que se harán auditorías periódicas del manejo de su usuario y clave.

- El Contratista conoce y acepta que la clave o claves asociadas a su nombre de usuario que sean utilizadas en sistemas de información de propiedad de la Corporación surtirán los mismos efectos que el de las firmas electrónicas establecidas en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, por lo que, tanto su funcionamiento como su aplicación se entenderán como una completa equivalencia funcional, técnica y jurídica.

El Contratista, de acuerdo a su nombre de usuario y clave asignados por la Corporación, podrá acceder a los activos de información en los que se le otorgó permiso.

El Contratista se compromete también a:

1. Informarse, entender, apoyar y cumplir con las Políticas, procedimientos y guías de Seguridad de Información y Tecnología de la Información Corporativas que gobiernan la protección, el uso y la operación de los activos de la información de la Corporación, en lo que aplique al motivo para el que fue contratado.
2. Hacer buen uso de los activos de información de la Corporación a los cuales tiene acceso para propósitos de cumplir con las tareas de trabajo a él asignadas.
3. Comprender que el usuario que le asignen y clave, para el acceso a cualquier sistema de información de la Corporación, son exclusivamente para su uso y para propósitos de su trabajo. Estar consciente que cualquier actividad en los sistemas, registrados con su usuario son de su responsabilidad, asumiendo en consecuencia todos los efectos que su uso cause.
4. Entender que la clave es un mecanismo importante para la protección de los sistemas y aplicaciones. Entender además, que su manejo es personal e intransferible y acuerda no divulgar la(s) clave(s) de acceso a él asignadas a ninguna persona, bajo ningún concepto, salvo el pedido escrito expreso de las autoridades de control interno, es decir: al Oficial de Seguridad de Información de la Corporación, el Administrador de Contrato o el Gerente General.
5. Estar consciente que se harán auditorías periódicas del manejo de su usuario y clave.

6. Informar al Administrador de Contrato y al Oficial de Seguridad de Información en la Corporación, cualquier anomalía, comportamiento o situación que pueda poner en peligro los activos de información de la Corporación.
7. Garantizar la confidencialidad, disponibilidad e integridad de la información en la Corporación; de ser necesario podrá extenderse y ser más puntual de acuerdo las actividades que demande el contrato.
8. La suscripción del presente instrumento implicará la aceptación de todas y cada una de las disposiciones y normas establecidas en el Ecuador sobre el manejo de datos electrónicos. Los términos y condiciones están sujetos a las disposiciones contenidas en la Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos, su Reglamento y las normas tributarias vigentes en el Ecuador.

Declaración

El Contratista conoce y acepta que la información que se procese, almacene, comunique, etc. a través de su dirección de correo electrónico_____; y las acciones que se generen mediante o en los sistemas informáticos de la Corporación, a través de su nombre de usuario asociado, son de su estricta responsabilidad.

El Contratista, acepta el usuario y clave que se le proporciona, la información que use, cree o edite, haciendo uso de los sistemas o medios electrónicos que se ponga a su disposición es de propiedad de la Corporación, de conformidad con lo establecido en el Contrato.

Duración

Este Compromiso de confidencialidad tendrá una duración indefinida a partir de la fecha de su suscripción por parte del Contratista, salvo para los activos de información perdieran el carácter de confidencial por haber sido revelados oficialmente al público por la CELEC EP.

Aceptación

Libre y voluntariamente, el Contratista declara su aceptación a todo lo establecido en el presente instrumento, sometiéndose a sus estipulaciones, y comprometiéndose a su estricto cumplimiento.

Fecha (dd/mm/aaaa): _____ / _____ / _____

f) _____

Representante legal: _____

No. Cédula Identidad: _____

Cargo: _____

GLOSARIO DE TÉRMINOS

- **Activos de Información:** activo que tiene algún valor para la Corporación y debe protegerse, de tal manera que un activo de información es aquel elemento que contiene o manipula información.
- **Clasificación de la información:** En relación con la información que se considere restringida, confidencial, pública, etc., se estará a las disposiciones contenidas en la Ley Orgánica de Transparencia y Acceso a la Información Pública LOTAIP.
- **Compromiso de Confidencialidad:** Es el instrumento legal mediante el cual el Servidor conoce, acepta y se somete a las políticas de confidencialidad y de manejo de la información de propiedad de CELEC EP, haciendo uso o no de los sistemas de información establecidos por la Corporación.
- **Control de accesos:** El acceso a la información y los procesos de negocio deben ser controlados sobre la base de los requerimientos de seguridad y de los negocios.
- **Incidente de Seguridad de la Información:** se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información.
- **Permisos:** o derechos de acceso para determinados usuarios y grupos de usuarios.
- **Servidor:** es una persona que en cualquier forma o a cualquier título, trabaje, preste servicios, o ejerza un cargo, función o dignidad del sector público.
- **Terceros:** Toda persona natural o jurídica cuyo patrono no sea la Corporación.

Sección V

Guía rápida de usuarios

SIC-GLG-002-2014

Revisión 1

Diciembre - 2014

CONTENIDO

INTRODUCCIÓN

El Equipo de Seguridad de Información de la Corporación ha creado la Norma Técnica de Seguridad de Información, misma que se acompaña de guías y un instructivo.
En ese conjunto de documentos, se mencionan todos los aspectos de Seguridad en los que la Corporación trabaja actualmente y se indica todas las responsabilidades de los Servidores y de la corporación para con los activos de información.
Esta guía rápida constituye un resumen de los puntos clave en cuanto a Seguridad de Información que todo Servidor debe conocer. Para mayor detalle por favor revise el Instructivo, Guías y Norma Técnica antes mencionados.
La Norma Técnica de Seguridad de Información está identificada con código SIC-NTE-001-2014. Las Guías existentes hasta el momento son:

- Control de acceso SIC-GCA-001-2014
- Contratos y compromiso de confidencialidad SIC-GLG-001-2014
- Guía rápida para usuarios SIC-GLG-002-2014
- Gestión de activos de información SIC-GAI-001-2014
- Gestión del cambio cultural SIC-GRH-001-2014
- Gestión de incidentes de seguridad de información SIC-GIS-001-2014
- Adquisición, desarrollo y mantenimiento de sistemas de Información SIC-GMS-001-2014

Las Normas Técnicas de Seguridad de Información comprenden un camino para mejorar el grado de madurez de la Corporación sobre la Seguridad de Información, por lo que su cumplimiento estará supeditado a una programación en base a prioridades y recursos destinados para su aplicación, conforme a lo señalado en el Instructivo de aplicación SIC-INS-001-2014.

1 IDENTIFICACIÓN Y AUTENTIFICACIÓN DE USUARIOS

h) Los usuarios serán creados conforme al procedimiento establecido en la Guía de control de acceso y serán activados posterior a la firma del Acuerdo de Confidencialidad.
i) Evitar el uso de usuarios genéricos. Cuando se requiera la creación de este tipo de usuarios, se enviará una solicitud a la Subdirección de Tecnologías de Información de Matriz; la solicitud debe realizarla de manera formal el Gerente de la Unidad de Negocio o el Director de

Gestión Estratégica en el caso de Matriz, adjuntando:

- Acuerdo de Confidencialidad suscrito por el Servidor que será responsable del manejo de la cuenta
- Justificación sustentada sobre la necesidad
- Formulario de creación de cuentas debidamente lleno

j) Los usuarios y contraseñas son personales e intransferibles, siendo el usuario dueño de la cuenta responsable de lo que se realice a través de su cuenta, con y sin su conocimiento.

2 CONTRASEÑAS

Los siguientes son los puntos más importantes del manejo de contraseñas que todos los Servidores deberán seguir. Aquí encontrará controles para su seguridad, complejidad y razones para bloqueo de las contraseñas.

e) El usuario deberá cambiar de manera obligatoria su clave la primera vez que ingresa a un sistema.
f) Se realizará una auditoría de contraseñas 2 veces al año.
g) Se cambiara de claves o contraseñas, cada 180 días para toda cuenta.
h) Los usuarios que tengan sospechas de que su contraseña es conocida por otra persona, deberán cambiarlas inmediatamente.
i) No se debe repetir las 3 contraseñas anteriores utilizadas en un servicio o sistema
j) No se debe revelar contraseñas de manera directa, por teléfono o respuesta a mensajes de correo electrónico.
k) No almacenar las contraseñas en programas gratuitos o pagados que tengan esta facilidad.
l) Las contraseñas no deben estar a disposición de terceros, de manera legible en medios impresos o físico, en caso de ser necesario su registro debe ser un lugar seguro y controlado.

2.1 Complejidad

d) Las contraseñas deben tener al menos ocho caracteres
e) Deben incluir:
    - Combinación de mayúsculas, minúsculas (desde A/a a la Z/z no Ñ/ñ).
    - Números (desde el 0 al 9)
    - Opcionalmente debe incluir caracteres no alfanuméricos (como #,”,@,%,$,&,/).

- No debe repetirse por lo menos 2 contraseñas anteriores en el mismo sistema o servicio.

f) No debe incluir nombres o apellidos del usuario, más de tres caracteres consecutivos.

2.2 Bloqueo

d) En los casos en que se impida el acceso, el administrador del servicio o sistema debe asignar una clave temporal al usuario.

e) Las cuentas de los sistemas de información de la Corporación se bloquean cuando:
   - Se introduce más de 3 veces seguidas la contraseña errónea. En este caso el bloqueo será temporal por 10 minutos, luego de lo cual será desbloqueada automáticamente. Este tipo de bloqueos puede repetirse solamente 2 veces seguidas, después de lo cual la cuenta quedará bloqueada hasta que se dirija una solicitud de desbloqueo al administrador.
   - Las cuentas que registren inactividad por 30 días sin aviso previo justificado.
   - El Servidor ha dejado de trabajar para la Corporación.

3 RESTRICCIÓN DEL CAMBIO DE PAQUETES DE SOFTWARE

a) Se debe disponer de la autorización del Subdirector o Jefe del área de Tecnologías de la Información y Comunicaciones para el cambio en la configuración del equipo. Los cambios en la configuración incluyen la instalación o eliminación de software.

4 TRASLADOS ADMINISTRATIVOS Y SEPARACIÓN DE LA CORPORACIÓN

a) El Servidor entregará los bienes y activos de información que están a su cargo, a las áreas correspondientes, de acuerdo a lo establecido en la Norma Técnica de Seguridad de Información y la Guía de Activos de Información.

5 RESPONSABILIDAD DEL SERVIDOR

a) La información que genere el Servidor, tales como programas, aplicaciones, planos, diagramas, cálculos u otros instrumentos que permitan mejorar procesos internos y automatización de tareas, son propiedad de la Corporación.
b) La conservación, buen uso y mantenimiento de los bienes, será responsabilidad directa del Servidor que los ha recibido para el desempeño de sus funciones y labores oficiales.
c) Guardar estricta reserva sobre la información de la Corporación catalogada como “Confidencial”.

6 CONTRATOS Y COMPROMISOS DE CONFIDENCIALIDAD

a) Todos los Servidores deben firmar el compromiso de confidencialidad de la Corporación.
b) Al realizar la contratación de un nuevo Servidor es necesario, que al firmar de su contrato se suscriba también el Compromiso de Confidencialidad, establecido por la Corporación.

7 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

a) Se debe informar sobre los incidentes de seguridad en activos de información conforme a lo establecido en la “Guía de gestión de incidentes de seguridad de información”, de manera inmediata.
b) El punto de contacto para reportar los eventos de seguridad de la información es la Mesa de Servicios.

Sección VI

Guía de gestión de activos de información

SIC-GAI-001-2014

Revisión 1

Diciembre - 2014

CONTENIDO

INTRODUCCIÓN

Esta guía define procesos y formatos que permitan realizar el inventario y clasificación de los activos de información de la Corporación, a fin de mantener un uso adecuado de los mismos y una apropiada gestión de los activos de información.

La realización del inventario y clasificación, nos ayuda a determinar el uso que se debe dar a los activos de información, en los procesos de la Corporación, reconociendo los niveles de confidencialidad que deben ser asignados, así como las responsabilidades que tienen los Servidores, frente a los mismos.

La presente guía, ha tomado como marco referencia la norma técnica internacional ISO27002:2013 en el ítem "8. Gestión de Activos", la Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27002:2009 en el ítem "7. Gestión de Activos" y "10.7 Manejo de los Medios" y el estándar NERC-CIP-002-4 Definición de Ciberactivos Críticos, para el levantamiento y clasificación de activos de información.

Posteriormente se podrá realizar el análisis de riesgos, determinando las vulnerabilidades y amenazas a las cuales se encuentra expuestos los activos de información identificados, para aplicar controles de seguridad mitigando las brechas de seguridad detectadas.

ALCANCE

- Obtener el inventario y clasificación de los activos de información, con su valor, tipo, ubicación y propietario, posterior análisis de riegos, según las normas y buenas prácticas de seguridad de información.
- Establecer el periodo de tiempo para la actualización del inventario de activos de información, verificar responsables y procesos a seguir para su tratamiento.
- Establecer un estándar para la gestión de activos de información.

OBJETIVO

- Mantener una gestión adecuada de los activos de información de la Corporación.
- Clasificar los activos de información según su naturaleza.

- Definir los responsables de cada uno de los activos de acuerdo a su clasificación.
- Valorar a los activos de información Corporativa en función a la confidencialidad, integridad y disponibilidad, base para la gestión de riesgos.

1 GESTIÓN DE LOS ACTIVOS DE INFORMACIÓN

Para la elaboración de la presente guía se analizaron las normas y estándares nacionales e internacionales logrando diseñar una metodología de gestión de activos de información, alineada a las mejores prácticas, adaptables a las necesidades y características de la Corporación.

El levantamiento de la información a ser utilizada para la elaboración del inventario y posterior clasificación de los activos de información para cada área y/o proceso de la Corporación, permite realizar una adecuada gestión de activos de información, conocer la sensibilidad al riesgo de cada activo e implementar planes de mitigación para eliminar o minimizar el riesgo.

La existencia, configuración, mantenimiento y estado de aplicabilidad de controles relacionados a la estrategia de Seguridad de Información en la Corporación, así como la posibilidad de uso a ambiente Corporativo de dichos controles, se debe informar al Oficial de Seguridad de Información.

1.1 Responsabilidad sobre los activos

1.1.1 Inventario de Activos

Todos los activos deben ser claramente identificados, para ello el Equipo de Seguridad de Información deberá elaborar y mantener un inventario de todos los activos de información, identificando el propietario y responsable de cada uno de ellos.

a) El inventario de los activos de información deberá contener datos como: nombre del activo, propietario, ubicación, tipo de activo, valor, responsable técnico. La persona responsable de gestionar los activos de información mantendrá actualizado el inventario constantemente.
b) La información será registrada en la “Matriz de inventario y clasificación de activos de información”, documento adjunto a la presente guía.

c) Los tipos de activos, detallados en el título 2 de la presente guía.
d) Los activos se pueden dividir en diferentes grupos según su naturaleza[9].
   - **Servicios:** Los procesos de negocio de la Corporación que ofrece al interno de la misma o a la ciudadanía. Como por ejemplo, servicios de internet, servicios de correo, servicio de telecomunicaciones, servicio de la cadena de suministros del sector eléctrico, servicios de integración entre aplicaciones, bases de datos (servicios web).
   - **Datos e Información de la Corporación:** aquellos que se e manipulan dentro de la Corporación. Base de datos, archivo de datos, documentación, manuales de usuario, contratos, acuerdos, normativas, procesos documentados, entre otros.
   - **Aplicaciones de Software:** software de aplicación, sistemas operativos, aplicativos desarrollado y en desarrollo, software del sistema, herramientas de desarrollo y utilitarios.
     1. Sistemas operativos.
     2. Software de servicio, mantenimiento o administración de gabinetes de servidores de cuchilla, servidores (estantería/rack, torre, virtuales), sistema de redes de datos, sistemas de almacenamiento (NAS, SAN), telefonía, sistemas (de UPS, grupo electrógeno, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión), entre otros.
     3. Paquetes de software o software base de suite de ofimática, navegador de Internet, cliente de correo electrónico, mensajería instantánea, edición de imágenes, vídeo conferencia, servidor (proxy, de archivos, de correo electrónico, de impresiones, de mensajería instantánea, de aplicaciones, de base de datos), entre otros.
     4. Aplicativos informáticos del negocio**.**
   - **Equipos Informáticos:** PC, portátiles, servidores, dispositivos móviles, medios removibles, etc.
     1. Equipos móviles: teléfono inteligente (Smartphone), teléfono celular, tableta, computador portátil, asistente digital personal (PDA), entre otros.
     2. Equipos fijos: servidor de torre, servidor de cuchilla, servidor de rack, computador de escritorio, computadoras portátiles, entre otros.

[9] Se ha hecho uso de Magerit para diferenciar los activos agrupándolos en varios tipo de acuerdo a la función que ejerce en el tratamiento de la información.

3. Periféricos de entrada: teclado, ratón, micrófono, escáner plano, escáner de mano, cámara digital, cámara web, lápiz óptico, pantalla de toque, entre otros.
4. Periféricos de salida: monitor, proyector, audífonos, parlantes, impresora láser, impresora de inyección de tinta, impresora matricial, impresora térmica, plotter, máquina de fax, entre otros.
5. Periféricos y dispositivos de almacenamiento: sistema de almacenamiento (NAS, SAN), librería de cintas, cintas magnéticas, disco duro portátil, disco flexible, grabador de discos (CD, DVD, Blu-ray), CD, DVD, Blu-ray, memoria USB, entre otros.
6. Periféricos de comunicaciones: tarjeta USB para redes inalámbricas (Wi-Fi, Bluetooth, GPRS, HSDPA, HSPA+, GSM, 5G), tarjeta PCMCIA para redes inalámbricas (Wi-Fi, Bluetooth, GPRS, HSDPA), tarjeta USB para redes alámbricas/inalámbricas de datos y de telefonía, entre otros.
7. Tableros: de transferencia (bypass) de la unidad interrumpible de energía (UPS), de salidas de energía eléctrica, de transferencia automática de energía, etc.
8. Sistemas: de control de accesos, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión, entre otros.

- **Redes de Comunicación:** aquellas que dan soporte a la Corporación para el movimiento y flujo de la información. Dispositivo de conectividad de redes como routers, switch, concentradores, entre otros.
  1. Cables de comunicaciones (interfaces: RJ-45 o RJ-11, SC, ST o MT-RJ, interfaz V35, RS232, USB, SCSI, LPT), panel de conexión (patch panel), tomas o puntos de red, racks (cerrado o abierto, de piso o pared), entre otros.
  2. Switchs (de centros de datos, de acceso, de borde, de gabinete de servidores, access-ppoint, transceiver, equipo terminal de datos, entre otros.).
  3. Ruteador (router), cortafuego (firewall), controlador de red inalámbrica, etc.
  4. Sistema de detección/prevención de intrusos (IDS/IPS), firewall de aplicaciones web, balanceadoras de carga, switch de contenido, entre otros.
- **Soporte de la información**: medios físicos que permiten el almacenamiento de la información, durante un largo período de tiempo.
- **Equipamiento auxiliar:** soporte a los sistemas de información, son aquellos que no se han incluido en ninguno de los grupos anteriores

(equipos de destrucción de información, equipos de climatización, UPS).

- **Instalaciones:** donde se alojan los sistemas de información oficinas, vehículos, entre otros.
- **Personal:** personal interno subcontratado, proveedores, etc.
- **Intangibles:** tales como reputación e imagen de la organización, estructura de organizacional:
    1. Estructura organizacional de la institución, que incluya todas las unidades administrativas con los cargos y nombres de las autoridades: área de la máxima autoridad, área administrativa, área de recursos humanos, área financiera, entre otros.
    2. Estructura organizacional del área de las TIC, con los cargos y nombres del personal: administrador (de servidores, de redes de datos, de respaldos de la información, de sistemas de almacenamiento, de bases de datos, de seguridades, de aplicaciones del negocio, de recursos informáticos, etc.), líder de proyecto, personal de capacitación, personal de mesa de ayuda, personal de aseguramiento de calidad, programadores (PHP, Java, entre otros.).
    3. Los procesos que solo hayan sido descritos por el Servidor y este no haya sido documentado, será considerado como un activo de conocimiento y este deberá ser recomendado para la creación de documentación y aprobación del mismo.

1.1.2 Responsables de los activos

a) Toda la información y activos asociados con los procesos de información deben ser asignados a Servidores de la Corporación, designados como Responsable del activo.
b) El Oficial de Seguridad de Información en conjunto con el Propietario de Activos de Información asignará los activos asociados (o grupos de activos) a un Servidor que actuará como Responsable.

El Responsable de activos de información, tiene como responsabilidades:

c) Orientar por el control de la producción, desarrollo, mantenimiento, uso y la seguridad de los activos, no implica que tendrá derechos de propiedad sobre los activos.
d) Consolidar los inventarios de los activos, informar al Oficial de Seguridad de Información del cuidado con los activos más críticos, que afecten a la integridad, disponibilidad y confidencialidad de la información provocando un impacto considerable al negocio Corporativo.

e) Mantener actualizado y documentado el inventario de los activos de información.
f) Notificar al Oficial de Seguridad, cualquier anomalía presentada en los activos de información inventariados.
g) Presentar trimestralmente al Oficial de Seguridad un informe sobre el estado y gestión de los activos de información.
h) Administrar la información dentro de los procesos de la Corporación a los cuales ha sido asignado.
i) Elaborar las reglas para el uso aceptable de los activos de información previa autorización de la autoridad correspondiente y posterior aprobación del Oficial de Seguridad de la Información.
j) Consolidar los inventarios de los activos a cargo del Responsable del Activo, por área o unidad organizativa.
k) Podrá delegar tareas rutinarias en caso de ser necesario, asumiendo su responsabilidad.
l) Todos las responsabilidades indicadas en la Norma Técnica, literal *1.1.6 Responsable de los activos de información.*

1.1.3 Uso aceptable de los activos

El Oficial de Seguridad de Información debe:

a) Identificar las reglas de uso aceptable de la información y los activos asociados con los servicios de procesamiento de la información, las mismas que deben ser documentadas e implementadas.
b) Definir las restricciones del uso de servicios de procesamiento y almacenamiento externo de la información con terceros.
c) Definir el nivel de impacto (Leve, Importante o Grave) a los sistemas y/o procesos de la Corporación en caso de ser conocido, utilizado o modificado el activo de información por alguna persona o sistema sin la debida autorización. Estos parámetros deberán ser considerados al momento de clasificar los activos de información.

El área de TIC deberá:

d) Asignar los equipos y se proceder con la activación de servicios informáticos necesarios para el desarrollo de sus funciones, al momento de la incorporación de un nuevo Servidor a la Corporación.
e) Asegurarse que cualquier activación de servicio, asignación de roles, creación de cuentas, entrega de equipos informáticos, se procesara el requerimiento previa aprobado de los Jefes inmediatos del Servidor solicitante, de ser necesario se solicitará un informe técnico.

El Propietario de la información, tiene como responsabilidades:

f) Controlar y determinar cuáles son los requisitos para que el activo de información sea salvaguardado ante accesos no autorizados, modificación, pérdida de la confidencialidad o destrucción deliberada, con el apoyo del Equipo de Seguridad de Información.
g) Controlar la dirección de la producción, desarrollo, mantenimiento, empleo y la seguridad del valor del activo, no significa que tenga derecho de propiedad sobre el activo.
h) Encargado del uso responsable de la información y a los activos que lo contienen sean estos digitales o físicos, como se indica en el "Reglamento General para el Manejo y Administración de Bienes del Sector Público"
i) Todos las responsabilidades indicadas en la Norma Técnica, literal *1.1.5 Propietarios de la información*.

1.1.4 Devolución de los activos

a) Una vez culminada la relación de dependencia del Servidor o tercero con la Corporación, deberán devolver todos los activos pertenecientes a la Corporación, que estén a su cargo, al momento de finalizar el contrato laboral, contrato, compromiso o acuerdo.
b) En los casos en que el Servidor o tercero usa su propio equipo, para desempeñar sus funciones, se debe asegurar que toda la información relevante es transferida a la Corporación y borrada del equipo.
c) Las áreas correspondientes deben verificar que los activos de información devueltos sean consistentes con los que inicialmente fueron asignados al Servidor.
d) En caso de que el Servidor termine su relación laboral o realice un cambio administrativo, el procedimiento será :
    - El Área de Talento Humano, notificará mediante memorando a las áreas correspondientes, la desvinculación o traslado de un Servidor, a fin de que se proceda con la devolución de todos los activos de información a su cargo.
    - Mediante un acta entrega-recepción suscrita por el área encargada de los inventarios de activos y TIC, quedará constancia de la devolución de los activos. Un original de esta acta será entregado al responsable de Gestión de Activos de Información.
    - En caso de que el Servidor no entregue el activo de información asignado en buen estado:
        - ✓ Área de TIC y el Área encargada de los inventarios de activos, deberán informar al Área de Talento Humano sobre los daños que posea el activo de información devuelto por el Servidor.

- ✓ En respuesta a la notificación emitida sobre los daños ocasionados al activo de información devuelto, procederá a ejecutar las acciones correctivas y sancionarías de acuerdo a lo establecido en el "***Reglamento Interno de Trabajo CELEC EP***".

2 CLASIFICACIÓN DE LA INFORMACIÓN

Todas las directrices de este punto deben ser seguidas por los Servidores a cargo de la clasificación de los activos, es decir, el Oficial de Seguridad de Información, el Equipo de Seguridad de Información, los Propietarios de los Activos de Información, los Responsables de los Activos de Información y en general los Servidores que de alguna manera manipulen o tengan contacto con los Activos de Información.

2.1 Directrices de Clasificación

a) En base a la identificación de los activos de información, se determinará la dependencia que existe entre ellos.
b) La información debe clasificarse de manera que permita demostrar las necesidades, prioridades y el grado esperado de protección al manejar la información.
c) Debe utilizar el esquema para la clasificación de la información, que permitan definir los niveles de protección adecuados.
d) Tomar en cuenta que la información tiene grados variables de sensibilidad y criticidad. Algunos elementos de información pueden requerir un nivel adicional de protección o un uso especial.
e) La clasificación de información, así como los controles de protección asociados a ellas, deben tener en cuenta las necesidades del negocio referente a compartir o restringir la información.

2.1.1 Valoración de los activos

a) Los criterios de valoración serán definidos en base a normas de seguridad, estándares de la industria, experiencia del entrevistador, buenas prácticas con resultados comprobados, tomando en cuenta el grado de importancia con relación al núcleo de negocio de la Corporación, y en función a estos tres parámetros principales: integridad, confidencialidad y disponibilidad.

b) La información deberá ser registrada en la “Matriz de inventario y clasificación de activos de información”, conforme a lo que indica esta guía, en especial los siguientes puntos:

2.1.1.1 Identificación

a) **Nombre Activo:** Se identificará al activo de información de manera particular y diferenciable dentro de la Corporación.
b) **Propietario:** Es el Servidor que tiene mayor conocimiento sobre el activo de información, y es el encargado de definir quien tiene acceso y que tramite dar a la información.
c) **Custodio Técnico:** Es el Servidor designado como RESPONSABLE y encargado de administrar y hacer efectivos controles de seguridad que el propietario de la información ha definido.
d) **Tipo:** los activos de información pueden pertenecer a los siguientes tipos: Servicio, Datos e información, Aplicaciones de Software, Equipos informático, Redes de Comunicación, Soporte de la información, Equipamiento auxiliar, Instalaciones, Personal, Intangible.
e) **Valor:** Indica el valor que tiene para la Corporación, dentro del proceso o área puede ser Critico, Alto, Medio o Bajo.
f) **Atributos de Calificación:** A cada activo de información se le relacionó uno o más atributos, los cuales permiten identificar su sensibilidad y justificar el valor asignado. Los atributos asociados al activo de información son los siguientes:

A1:	El activo de información debe protegerse de terceros.
A2:	El activo de información debe ser restringido a un número limitado de Servidores.
A3:	El activo de información debe ser restringido a personas externas.
A4:	El activo de información puede ser alterado o comprometido por fraudes o corrupción.
A5:	El activo de información es muy crítico para las operaciones internas.
A6:	El activo de información es muy crítico para los servicios hacia terceros.
A7:	El activo de información ha sido declarado de conocimiento público, por la SNAP o alguna norma jurídica
A8:	Causaría perjuicio a la Corporación no saber exactamente que se hace o se ha hecho con el activo de información
A9:	El conocimiento del activo de información, por parte de una persona que no debe saber de su existencia, causaría un daño importante a la Corporación
A10:	Si el activo de información se encuentra dañado o corrupto, causaría daño a la Corporación
A11:	Causaría daño no saber a quién se le ha asignado acceso al activo de información
A12:	Causaría daño al activo de información, no saber quién accede a qué datos y que

hacen con ellos

A13: Si el activo de información queda inhabilitado, ¿cuál sería el tiempo de tolerancia para su funcionamiento nuevamente? (minutos, horas, semanas, meses)

A14: ¿Cuál considera Usted, son los componentes más importantes del activo de información?

A15: Qué componente del activo de información, tendría que ser afectado para realizar un ataque

g) **Acceso:** Se identificará que usuarios tienen accesos con o sin autorización para hacer uso de la información. Los derechos de acceso pueden ser: (L) lectura, (E) Escritura, (M) Modificación, (B) Borrado o eliminación.
h) **Ubicación:** Información acerca de donde se encuentra específicamente ubicado el activo de información, puede ser un archivo físico de oficina, archivo digital, sistema de información, computador, base de datos, o aplicación. Para ello se deberá indicar si el activo se encuentra disponible en medio físico o en medio electrónico.
i) **Grado de Dependencia**: Relación que tiene el activo de información con los sistemas informativos, procesos de la Corporación.

2.1.1.2 Niveles de Clasificación

a) **Pública:** En atención a La Ley de Transparencia y Acceso a la Información Pública LOTAIP, en su Art.7, se dará cumplimiento a esta ley para dar a conocer al ciudadano en general la información de la Corporación: Propaganda, Boletines de Prensa, Comisiones, entre otros.
b) **Confidencial:** Aquella información donde su divulgación no autorizada puede derivar en impactos importantes para la Corporación. Ejemplo: presupuestos, nómina y compensaciones, reportes de auditoría, contraseñas, entre otros.
c) **Uso Interno**: Aquella información que apoya a los procesos internos y que no ha sido clasificada como restringida ni confidencial, por lo que puede ser conocida dentro de toda la Corporación. No puede ser difundida a proveedores ni a terceros. Su divulgación no autorizada representa un impacto menor para el negocio. Ejemplo: Comunicados Internos, Organigramas, Manuales de procedimientos.
d) **Restringida:** Aquella información privilegiada en donde su divulgación no autorizada puede derivar en impactos financieros, legales, con la ciudadanía, proveedores, gobierno entidades externas, operaciones y transacciones. Ejemplo: Planes Estratégicos, Estados Financieros, Datos de adquisiciones (antes de su anuncio), Negociaciones con

proveedores, Desarrollo de nuevos servicios, Juicios, Concursos internos, entre otros.

2.1.1.3 Criterios de valoración

a) Los activos de información, tienen atributos como Confidencialidad, Integridad y Disponibilidad, representados con características en el rango de Bajo, Medio, Alto, Critico, que nos permite estimar el nivel de criticidad de cada activo de información identificado.
b) La información de los criterios de valoración nos permite indicar el valor que tienen para la Corporación. A continuación se detalla el significado de cada rango:

Confidencialidad

Valor del activo	Descripción
Bajo	El conocimiento o divulgación de la información pública no autorizada no tiene ningún impacto negativo en el proceso
Medio	Información se restringe al uso interno, en función a las necesidades del negocio, y requerimientos de cada área.
Alto	El conocimiento o divulgación de información de uso interno afecta financieramente a la Corporación.
Crítico	El conocimiento o divulgación de información confidencial no autorizada impacta negativamente a la Corporación, de manera financiera y operacionalmente.

Tabla 1. Criterios de Confidencialidad

Integridad

Valor del activo	Clasificación	Descripción
Bajo	Integridad Baja	El daño o modificación no autorizada de información así como a pérdida de exactitud y métodos de procesamientos, no tiene ningún impacto negativo en el proceso, ni implicaciones críticas para las aplicaciones del negocio y su impacto es insignificante o menor.
Medio	Integridad Media	El daño o modificación no autorizada a la información no es crítica pero es sensible a las aplicaciones y el impacto en el negocio es importante.
Alto	Integridad Alta	El daño o modificación no autorizada de la información es fundamental para las aplicaciones del negocio y el impacto es importante, podría dar lugar a infracciones

		graves de las aplicaciones de negocio.
Crítico	Integridad Muy Alta	La pérdida de exactitud y estado completo de la información y métodos de procesamientos impacta negativamente a la Corporación.

Tabla 2. Criterio de Integridad

Disponibilidad

Valor del activo	Clasificación	Descripción
Bajo	Disponibilidad Baja	El activo de información ((información, procesamiento de la información, los recursos del sistema / servicios de conexión, personal, entre otros) puede no estar disponible por 8 horas (un día de trabajo), sin que esto afecte a los procesos apoyo internos y externos de la Corporación, esto no incluye a los procesos del giro del negocio.
Medio	Disponibilidad Media	El activo de información ((información, procesamiento de la información, los recursos del sistema / servicios de conexión, personal, entre otros) puede no estar disponible máximo medio día, sin que esto afecte a los procesos de apoyo internos y externos de la Corporación, esto no incluye a los procesos del giro del negocio.
Alto	Disponibilidad Alta	El activo de información (información, procesamiento de la información, los recursos del sistema / servicios de conexión, personal, entre otros) puede no estar disponible por 3 horas, sin que esto afecte a los procesos de apoyo internos y externos de la Corporación, esto no incluye a los procesos del giro del negocio.
Crítico	Disponibilidad Muy Alta	La falta del activo de información impacta negativamente a la Corporación El activo de información ((información, procesamiento de la información, los recursos del sistema / servicios de conexión, personal, entre otros) debe estar siempre disponible las 24 horas, los 365 días, ya que afecta a los procesos internos y externos del giro del negocio de la Corporación, y puede ser sancionada por organismos regulatorios.

Tabla 3. Criterios de Disponibilidad

c) De existir diferentes tiempos valores diferentes a los indicados en las Tablas 3, para los tiempos en los cuales un activo de información está fuera de servicio, se debe indicar en el campo *"Observaciones"* de la Matriz de inventario y clasificación de activos de información.

d) Identificado los requisitos de cada parámetro de la calificación de los activos de información, se procederá a la asignación de valores:

	Valor		Criterio
10	C	Crítico	Daño muy grave para la Corporación.
7-9	A	Alto	Daño grave a la Corporación
4-6	M	Medio	Daño importante a la Corporación
1-3	B	Bajo	Daño menor a la Corporación

Tabla 4. Criterio de Valoración de Activos

e) La clasificación que obtendrá cada activo de información se generara en base a la valoración obtenida en confidencialidad, disponibilidad e integridad, quedando definida del a siguiente manera:

COMBINACIONES			RESULTADO FINAL
CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	
C	C	C	Confidencial/Restringido
C	C	M	Confidencial/Restringido
C	C	B	Confidencial/Restringido
C	C	A	Confidencial/Restringido
A	A	A	Confidencial/Restringido
A	A	M	Confidencial/Restringido
A	A	B	Confidencial/Restringido
A	A	C	Confidencial/Restringido
M	M	M	Uso interno
M	M	C	Confidencial/Restringido
M	M	B	Uso interno o pública
M	M	A	Uso interno

B	B	B	Uso Interno
B	B	A	Uso Interno
B	B	C	Confidencial/Restringido
B	B	M	Uso interno

f) Es importante tomar en cuenta que, si la información es privilegiada y confidencial, esta deberá considerarse como restringida.
g) Si la información no es privilegiada, pero es considerada importante en caso de que terceros tengan acceso a la misma y cause un gran impacto a la Corporación será considerada como confidencial.
h) La información sobre los activos de información, serán registrados en forma digital y validada su existencia en forma física, quiere decir que existirá consistencia tanto en el inventario de los activos de información del Área de TIC con el de Bienes.
Existirá un registro que constate la entrega del bien al usuario.

2.2 Etiquetado y manipulado de los activos información

a) Los activos que no deberán poseer la etiqueta de seguridad de la información son los bienes muebles, solamente contaran con le etiqueta de control de bienes.
b) Los activos de información deben contar con un manejo y etiquetado que se encuentre acorde a la clasificación de cada uno de ellos, garantizando su confidencialidad, integridad y disponibilidad.
c) Los activos de información que fueron clasificados, deben incluir el siguiente etiquetado para su manejo, almacenamiento, procesamiento, transmisión y destrucción.

Clasificación	**Descripción**
Activo de la Información Pública	El conocimiento o divulgación no autorizada de este activo de información no tiene ningún impacto negativo en el proceso. Información no sensible y acceso a instalaciones, procesamiento de la información y sistemas a disposición del público.
Activo de la Información Interna	Información se restringe al uso interno, en función a las necesidades del negocio.
Activo de la Información Confidencial	Información sensible. Las instalaciones de procesamiento de la información están basadas en el concepto “necesidad de conocer”
Activo de la Información	El conocimiento o divulgación no autorizada de este activo de información impacta negativamente a la Corporación.

Restringida	

d) Incluir datos mediante abreviaturas, acerca del tipo de activo y su funcionalidad para la generación de etiquetas, en caso de repetirse la etiqueta del activo, deberá añadirse un número secuencial único al final.
e) Las etiquetas generadas deberán estar incluidas en el inventario, asociadas a su respectivo activo.
f) Los responsables de los activos supervisarán el cumplimiento del proceso de generación de etiquetas y rotulación de los activos.
g) Para el caso de etiquetas físicas, los responsables de los activos verificarán con una periodicidad no mayor a 6 meses, que los activos se encuentren rotulados y con etiquetas legibles.
h) En caso de destrucción de un activo, la etiqueta asociada a éste debe mantenerse en el inventario respectivo con los registros de las acciones realizadas.
i) Los documentos, procesos, manuales, informes y demás activos que generen información, que contengan datos del tipo “restringida” deben ser etiquetados como tal. La copia o transferencia por cualquier medio (electrónico, magnético, en papel) de información “restringida” debe estar autorizada y controlada. Todos los documentos del tipo “restringida” y “confidencial” deben conservarse bajo llave.
j) La información sensible se debe reflejar por medio de una etiqueta apropiada, la clasificación a la que pertenece, sin importar la forma o medio en la que se encuentre.

2.3 Manipulación de activos de información

a) El Equipo de Seguridad de Información y el Responsable de activo de información, deben elaborar procedimientos para el manejo, procesamiento, almacenamiento y comunicación de la información de acuerdo con su clasificación.
b) El envío de documentos con esta clasificación, debe hacerse por medio de canales seguros información tales como mensajería privada, correo electrónico encriptado, entrega personal. Es importante evitar el uso del servicio postal, fax, internet o medios no controlados para su envío.
c) Toda recepción de información sensible, debe acusar formalmente como recibida.
d) El envío físico de información sensible debe hacerse por medio de paquetes debidamente cerrados y que no permitan observar su contenido.
e) La información del Sector que se utilice para ofrecer conferencias, discursos o presentaciones abiertas debe llevar la autorización del

propietario de la información y En su caso, de la Unidad de Negocio y Departamento de pertenencia.

f) Los administradores de aplicaciones deben garantizar que los datos de entrada están completos, que el procesamiento se lleva a cabo correctamente y sin interrupciones y se valide las salidas.

3 MANEJO DE SOPORTES DE ALMACENAMIENTO

3.1 Gestión de soportes extraíbles

a) Los soportes extraíbles incluyen cintas, disco, memorias de almacenamiento, unidades de almacenamiento removibles, disco compactos, disco de video digital y medios impresos.[10]
b) Todos los medios que contengan información importante para la Corporación deben ser almacenados en un ambiente seguro, y con vigilancia de acuerdo a su grado de criticidad.
c) El área de abastecimientos y el área de TIC deben contar con un registro de los medios extraíbles, con la finalidad de evitar la pérdida de datos debido a una sustracción, o robo de los medios.
d) El área de TIC y/o los Administradores o Responsables de los Centros de Operación y Control deberán verificar la posibilidad que los medios extraíbles sean activados solo si existe una razón de negocio para hacerlo, para evitar fuga de información.

3.2 Eliminación de soportes

a) Se debe considerar un centro de destrucción de documentos restringidos o confidenciales que garantice la no reutilización de la información.
b) La destrucción de registros e información de la Corporación debe ser formalmente autorizada por la Gerencia.
c) Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por el Organismo.
d) Los procedimientos para la seguridad de los medios que contienen información sensible deben ser implementados de acuerdo a la

[10] Tomado NTE INEN-ISO/IEC 27002:2005

sensibilidad de dicha información. Se deberían considerar los siguientes puntos:

- ✓ Identificar los medios que requieran eliminación segura.
- ✓ Almacenar y eliminar de forma segura los medios que contienen información sensible, como la incineración, trituración o borrado de los datos.
- ✓ Establecer procedimientos para selección del contratista que ofrece servicios de recolección y eliminación del papel, equipos y medios.
- ✓ Registrar la eliminación de los medios para mantener pruebas de auditoría.

4 DIFUSIÓN

a) Este documento será difundido a los miembros del Equipo de Seguridad de la Información Corporativa, a fin de que se pueda realizar el levantamiento, inventario y clasificación de los activos de información.
b) El presente documento también se pondrá en conocimiento, de las áreas relacionas con Talento Humano y Abastecimiento.
c) El Equipo de Seguridad de Información Corporativa, deberá modificar y actualizar la *"Guía de Gestión de Activos de Información"*, mantendrán reuniones con los involucrados para estandarizar y mejorar los procesos en la Matriz y las Unidades de Negocio.
d) Las áreas de TIC, serán quienes difundan las mejoras realizadas a la presente guía, por parte de los involucrados.

GLOSARIO DE TÉRMINOS

- **Información:** Es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada.[11]
- **Inventario:** Registro documental de bienes y activos de información.
- **Proceso:** Conjunto de actividades o eventos, que transforman elementos de entrada en resultados.
- **Proceso** Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados[12]
- **Trazabilidad:** Las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

[11] Tomada de NTC ISO/IEC 17799-2005

[12] Tomada de NTC ISO/IEC 9000

Sección VII

Guía de gestión del cambio cultural

SIC-GRH-001-2014

Revisión 1

Diciembre - 2014

CONTENIDO

INTRODUCCIÓN

La guía de sensibilización sobre seguridad de la información, pondrá en práctica iniciativas de sensibilización dirigidas a diferentes grupos de Servidores en la Corporación.

El cumplimiento de la sensibilización sobre seguridad de la Información en la Corporación, es de vital importancia para formar una adecuada cultura organizacional sobre la aplicación de buenas prácticas de seguridad.

OBJETIVO

- Aplicar la sensibilización de la información en la Corporación.
- Utilizar métodos que permitan concientizar al usuario, aplicar el buen uso de la seguridad de la información en la Corporación.

ALCANCE

Desarrollar la guía para aplicación de la sensibilización sobre seguridad de la información en la Corporación, a través de programas y métodos. Para ello se realizará un análisis que permita determinar el tipo de grupos de Servidores que existen en la Corporación. A fin de cambiar la cultura organizacional de la Corporación e instruir al Servidor , sobre las buenas prácticas de seguridad de la información.

1 ESTRATEGIAS PARA REALIZAR PROGRAMAS DE SENSIBILIZACIÓN

1.1 Planificación y valoración

a) El Equipo de Seguridad de Información en coordinación con el área de Comunicación Corporativa se encargará de planificar y organizar la iniciativa para la aplicación de tareas que permitan para lograr la sensibilización a los usuarios sobre la seguridad de la información en la Corporación. El encargado deberá poseer un comunicación abierta, honesta, clara y oportuna.
b) Previo a ejecutar un programa de sensibilización, se deberá contar

con el presupuesto que permita patrocinar el programa. Para ello se deberá presentar oportunamente un cronograma que contenga el plan de sensibilización y demás recursos.

c) El Oficial de Seguridad de Información aprobará el Plan de Gestión de Cambio y solicitará una autorización al Gerente General para ejecutar acciones del plan que se consideren de alto riesgo.
d) El Oficial de Seguridad de Información designará del Equipo de Seguridad de Información un responsable del programa de sensibilización.
e) El responsable del programa de sensibilización, deberá:
    - Establecer el alcance, metas, criterios de evaluación para ejecutar la sensibilización.
    - Mantenerse en iniciativa constante.
    - Evaluar si el mismo puede ser realizado con un profesional interno de la Corporación o si se requiere contratar de manera externa.
    - Definir adecuadamente los usuarios a los que estará dirigido estos programas.
    - Considerar que, si la lista de temas sobre seguridad de la información es larga, es conveniente, organizar el programa en secciones distribuidas a lo largo del tiempo.
    - Difundir a los usuarios de la Corporación el programa de sensibilización, utilizando canales de comunicación Corporativos, tales como: correo electrónico, vía telefónica, carteleras, folletos, revistas, anuncios en el sitio web de la Corporación, encuestas internas, salvapantallas, videos, etc.
f) Una vez desarrollada una lista completa de los temas que abarcará el programa de sensibilización , deberán ser evaluados y clasificados por orden de importancia, con el objeto de concentrarse en los temas más importantes para definir y precisar los requisitos del programa de sensibilización.

1.2 Fases para sensibilizar la información en grupos

Por regla general es necesario identificar grupos específicos que tengan intereses y prioridades similares, para lo cual:

a) El responsable del programa de sensibilización deberá identificar los grupos existentes en la Corporación, a fin de realizar una sensibilización eficaz y eficiente.
b) El responsable de la sensibilización podrá aplicar las siguientes fases

que le permitirán realizar un análisis de los grupos destinatarios.

- **Seleccionar los grupos destinarios:** Los grupos destinatarios son los afectados por el conocimiento de las cuestiones relacionadas con la seguridad de la información o pueden influir sobre dicho conocimiento.
- **Comprender la situación:** Los grupos destinatarios pueden estar preocupados por los efectos en su organización, la pérdida de control, etc.
- **Evaluar el nivel de conocimientos:** Asignar una calificación A (alta), M (media) o B (baja) que refleje el conocimiento de cada grupo destinatario sobre las cuestiones relacionadas con la seguridad de la información y sobre las soluciones que existen.
- **Determinar los comportamientos deseados:** Definir la conducta que debe adoptar cada grupo destinatario para resolver los principales problemas.

c) Una vez determinado los grupos se procederá a sensibilizar la seguridad de la información en la Corporación.

d) La siguiente matriz se utilizará como método para llevar a cabo las tareas antes mencionadas:

Objetivos de la Comunicación				
Grupo destinatario	Sensibilizar	Ayudar a comprender	Mejorar los conocimientos	Buscar soluciones
Grupo 1				
Grupo 2				
……..				
Metas y tipos de canales de comunicación	*Sitio web, correo electrónico, folletos, etc.*	*Presentaciones, reuniones, charlas, video conferencias, conferencias, etc.*	*Talleres, Sesiones de preguntas y respuestas, etc.*	*Memorandos, capacitaciones, talleres, etc.*

Tabla 1: Objetivos de la Comunicación

2 EJECUCIÓN Y GESTIÓN

a) Una vez aprobado el plan de sensibilización para la Corporación el responsable del programa de sensibilización lo deberá poner en marcha.

b) Al ejecutar el plan de sensibilización en cada Unidad de Negocio y Matriz, el responsable del programa presentará informes del cumplimiento al Oficial de Seguridad para su control y seguimiento.

3 EVALUACIÓN Y MODIFICACIÓN

El responsable de sensibilización deberá:

a) Realizar una evaluación de la eficacia y eficiencia del programa y su capacidad de mejorar la seguridad de la información en la Corporación.
b) Aplicar cuestionarios de seguimiento a fin de evaluar el alcance y el nivel de comprensión del programa de sensibilización difundido.
c) Determinar qué ha logrado la sensibilización, si ha sido beneficiosa para la Corporación, si ha sido comprendida fácilmente por el usuario, qué se debe hacer para lograr los resultados esperados y si es necesario modificar objetivos.
d) Mejorar el programa inicial, cuanto no haya resultado del todo, de tal manera que se cubran todos los requerimientos sobre seguridad de la información que la Corporación demanda.
e) Trabajar solamente con la última versión, en caso de existir una retroalimentación del plan de sensibilización debido a las actualizaciones de TI, procesos, servicios, aplicaciones, nuevos servicios, etc.

El Oficial de Seguridad de Información deberá:

f) Analizar los resultados y conclusiones obtenidas en los informes de sensibilización.

4 CONSIDERACIONES GENERALES

El responsable del plan de sensibilización deberá asegurarse que se incluya en él herramientas, métodos y recursos para sensibilizar sobre:

a) El contenido de las pantallas de los equipos, con el fin de que no se encuentren iconos y accesos innecesarios, y carpetas y archivos que deben ubicarse en la carpeta de documentos del usuario.
b) Mantener bajo llave la información sensible (cajas fuertes o

gabinetes), en especial cuando no estén en uso y no se encuentre personal en la oficina.

c) Desconectar de la red, servicio o sistema, las computadoras personales, terminales, impresoras asignadas a funciones críticas, cuando se encuentren inactivas.
d) Proteger los puntos de recepción de correo postal y fax cuando se encuentren desatendidas.
e) Bloquear las copiadoras y disponer de un control de acceso especial para horario fuera de oficinas.
f) Retirar información sensible una vez que ha sido impresa.
g) Retirar información sensible, como las claves, de sus escritorios y pantallas.
h) Retirar los dispositivos informáticos que estén sin uso.
i) Considerar todos los activos de información como los discos duros de los computadores personales (escritorio, portátiles, etc.) y otros dispositivos que se considere necesarios, de las máximas autoridades de la Corporación.
j) En el proceso de sensibilización, se deberá concientizar al personal sobre:
    - Toma de debidas precauciones, por ejemplo no revelar información sensible como para evitar ser escuchado o interceptado, al hacer una llamada telefónica.
    - Recordar al personal que no sostengan conversaciones confidenciales en lugares públicos u oficinas abiertas y lugares de reunión con paredes delgadas.
    - No dejar mensajes en contestadores automáticos puesto que éstos pueden ser escuchados por personas no autorizadas, almacenados en sistemas públicos o almacenados incorrectamente como resultado de un error de discado.
    - Recordar al personal los problemas ocasionados por el uso de máquinas de fax, con el acceso no autorizado a sistemas incorporados de almacenamiento de mensajes con el objeto de recuperarlos.
    - La programación deliberada o accidental de equipos para enviar mensajes a determinados números.
    - El envío de documentos y mensajes a un número equivocado por errores de discado o por utilizar el número almacenado equivocado

GLOSARIO DE TÉRMINOS

- **Cultura organizacional**: son expresiones utilizadas para designar un determinado concepto de cultura (el que la entiende como el conjunto de experiencias, hábitos, costumbres, creencias, y valores, que caracteriza a un grupo humano) aplicado al ámbito restringido de una organización, administración, corporación, empresa, o negocio.
- **Grupos destinatarios**: Servidores a quienes están dirigidos los programas de sensibilización.
- **Programas**: se refiere a las actividades, métodos, cronograma para preparar y ejecutar la sensibilización en la Corporación.
- **Puestos de trabajo**: lugar o espacio físico donde se encuentra un Servidor para realizar su trabajo diario.
- **Sensibilizar**: lograr que una persona conozca y se dé cuenta de la importancia o el valor de uno o varios temas.

Sección VIII

Guía de gestión de incidentes de seguridad de la información

SIC-GIS-001-2014

Revisión 1

Diciembre - 2014

CONTENIDO

INTRODUCCIÓN

Una serie de ocurrencias o eventos en un sistema o servicio, no deseados o inesperados que afectan las operaciones del negocio y amenazan la seguridad de la información es conocido como un Incidente de Seguridad de la Información.

La comunicación de los eventos relacionados con la seguridad de la información, nos permite garantizar que las causas, los procedimientos y la solución a dichos eventos sean utilizadas para la implementación de acciones correctivas y preventivas oportunas.

Para una correcta Gestión de Incidentes es necesario establecer las responsabilidades y los procedimientos de gestión que permitan dar una respuesta oportuna, efectiva y ordenada a los incidentes en la seguridad de información.

Los Servidores que en el ejercicio de sus funciones diarias manipulen información de cualquier tipo, deberán garantizar su confidencialidad, integridad y disponibilidad.

ALCANCE

Establecer una guía para el manejo de incidentes de seguridad que comprometa la confidencialidad, integridad o disponibilidad de la información o de los sistemas.

Entre los incidentes que pueden afectar a un servicio, operación o sistema se encuentran:

- Ataques de denegación de servicios.
- Código malicioso.
- Accesos no autorizados.
- Mal uso de recursos o sistemas.
- Scanning o pruebas no autorizadas a la red.
- Ataques a los componentes de la red.

OBJETIVO

- Elaborar un guía para la gestión de incidentes, que permita identificar y planificar eficientemente acciones, canales de comunicación, responsabilidades y aplicación de mitigaciones.

- Adoptar las medidas de seguridad de manera eficiente para proteger los activos de información, de la Corporación.

1 NORMAS GENERALES

a) Todos los Servidores, incluidos proveedores, contratistas y usuarios de terceras partes deberán informar de manera inmediata a la Mesa de Servicios, sobre los incidentes de seguridad ocurridos sobre los activos de información, para que se tomen las medidas correctivas y preventivas del caso, de manera inmediata.
b) El Oficial de Seguridad, trabajando en conjunto con el Equipo de Seguridad, definirá los procesos, procedimientos a fin de contar con un estándar para la gestión interna de los incidentes de seguridad.
c) La prioridad de los incidentes, está determinada por su impacto a los procesos del negocio, número de usuarios afectados, y el tiempo utilizado para la resolución del incidente y los niveles de servicio.
d) El Equipo de Seguridad de Información debe aplicar actividades proactivas como el análisis de alertas y amenazas, actividades de sensibilidad, definición de procedimientos, análisis y mejora continua de procesos.
e) El Operador de Seguridad, el Equipo de Seguridad de la Información o el Oficial de Seguridad de Información (según corresponda de acuerdo a la prioridad y clasificación del incidente) deberá tomar las medidas pertinentes para prevenir o eliminar las vulnerabilidades o debilidades detectadas.
f) El Oficial de Seguridad, mantendrá comunicación con los organismos durante la ocurrencia de un incidente y conformar equipos de trabajo a efectos de recuperar la información afectada y analizar el incidente.
g) El Operador de Seguridad, el Equipo de Seguridad de la Información y el Oficial de Seguridad de Información, deberá guardar reserva acerca de la información relativa a incidentes de seguridad informática de acuerdo a la normativa vigente.
h) El Equipo de Seguridad de Información deberá 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 que amenace la seguridad de la información, estableciendo como punto de contacto la Mesa de Servicios a fin de reportar los eventos de seguridad de la información.

2 REPORTE DE EVENTOS DE SEGURIDAD

a) Se establece como punto de contacto para el reporte de los eventos de seguridad de la información a la Mesa de Servicios, quien a su vez comunicará al Equipo de Seguridad de Información.
b) Todos los incidentes de seguridad de la información deben ser registrados, asignados, solucionados y se debe mantener un histórico de todo lo relacionado con el incidente desde su registro; este registro lo realizará la Mesa de Servicios y a el tendrá acceso el Equipo de Seguridad de Información, el Operador de Seguridad y el Oficial de Seguridad de Información.
c) Además de la bitácora de registro de incidentes y el reporte de vulnerabilidades de la seguridad de la información, el monitoreo de los sistemas, las alertas y las vulnerabilidades, se deberá establecer y ejecutar un procedimiento para la gestión de incidentes.
d) El Equipo de Seguridad de Información debe trabajar para que el punto de contacto sea conocido en toda la Corporación, y suministre respuestas oportunas y adecuadas.
e) Se debe reportar la fecha, hora, apellidos y nombres del funcionario que detectó la debilidad o vulnerabilidad, descripción de la debilidad, descripción de posibles incidentes de seguridad que pudieran ocurrir producto de esta debilidad.
f) El registro se realizara en una bitácora de incidentes (reporte de eventos) incluyendo fecha, hora, nombres y apellidos del funcionario en turno, departamento o área afectada, equipo o sistema afectado y breve descripción del incidente.

3 CLASIFICACIÓN DE INCIDENTES

a) El Equipo de Seguridad de Información deberá clasificar el incidente de acuerdo al tipo afectación del servicio y al nivel de severidad.
    - Por tipo de afectación entendemos a una clasificación en categorías que cataloguen los aspectos funcionales del incidente. Como acceso no autorizado a sistemas,

denegación de servicio, divulgación de información sensible, infección de malware, entre otros.

- Por nivel de severidad se comprende la clasificación en base al impacto puede ser medido por escala monetaria, escala de impacto funcional, afectación de los servicios, entre otros.

4 ACCIONES PARA ATENDER UN INCIDENTE

El Equipo de Seguridad de Información deberá:

a) Identificar el incidente de seguridad, determinar el alcance y los sistemas afectados.
b) Realizar un diagnóstico inicial, determinando mensajes de error producidos, identificando los eventos ejecutados antes de que el incidente ocurra, recreando el incidente para identificar sus posibles causas.
c) Asignar una prioridad de atención al incidente en el caso de que se produjeran varios en forma simultánea.
d) Trabajar con el área de TIC y el área afectada para el aislamiento de sistemas y procesos del negocio afectados.
e) El responsable de llevar éste reporte denominado "Reporte de vulnerabilidades o debilidades de la seguridad de la información" es el Oficial de Seguridad de Información.

5 RECOLECCIÓN DE EVIDENCIAS

El Equipo de Seguridad de Información deberá:

a) Asegurar que los sistemas de información cumplan con las normas legales para la producción de evidencia y así lograr la admisibilidad, calidad y cabalidad de la misma
b) Identificar y analizar las posibles causas de un incidente producido.
c) Desarrollar y cumplir procedimientos internos cuando se recolecta y se presenta evidencia con propósitos de acción disciplinaria dentro de la Corporación.
d) Garantizar la calidad y consistencia en la evidencia en todo el proceso.
e) Registrar los custodios mediante un rastreo sólido de la evidencia, para la recuperación, almacenamiento y procesamiento.

f) Tomar duplicados o copias de todos los medios removibles, utilizando mecanismos que no afecten al dispositivo original, la información de discos duros o memorias debe garantizar la disponibilidad; es conveniente conservar el registro de todas las acciones durante el proceso de copiado y dicho proceso debería tener testigo.
g) Conservar los dispositivos originales intactos y de forma segura..
h) Proteger la integridad de todo el material de evidencia. El proceso de copia del material de evidencia debe estar supervisado por un especialista designado por el Oficial de Seguridad de Información y se debe registrar la información sobre cuándo y cómo se realizó dicho proceso, quién ejecutó las actividades de copiado y qué herramientas o programas se utilizaron (cadena de custodia).
i) Recolectar y asegurar pistas de auditoría y toda la evidencia relacionada con el incidente.

6 INFORMES DE GESTIÓN DE INCIDENTES

El Equipo de Seguridad de Información deberá:

a) Generar un informe formal para el reporte de los eventos de seguridad de la información, en el que se contemple escalamiento y respuesta ante el incidente, que establezca la acción que se ha de tomar al recibir el reporte sobre un evento que amenace la seguridad de la información.
b) Elaborar y difundir recomendaciones, buenas prácticas y estándares en materia de protección de activos de información críticos, mediante el “Plan de Gestión de Cambio” que el Equipo de Seguridad de Información realizará conforme a la “Guía de gestión de cambio cultural”.

6.1 Aprendizaje debido a los incidentes de seguridad de la información

El Equipo de Seguridad a cargo de la administración de incidentes, deberá y presentará un informe de incidentes mensualmente al Oficial de Seguridad que contenga:

a) Determinar el número de incidentes por tipo, el número de incidentes graves, el tiempo medio de resolución de incidentes.
b) Determinar el costo promedio por incidente.

c) Determinar el número de incidentes recurrentes.
d) Determinar la frecuencia de un incidente recurrente.

7 RESTRICCIONES

a) Ningún Servidor deberá probar una debilidad o vulnerabilidad detectada en la seguridad de información, pues se interpretará como un uso inadecuado del sistema, equipo o servicio. Esto podría causar daño al sistema o servicio de información y eventualmente podría recaer en una responsabilidad legal.

GLOSARIO DE TÉRMINOS

- **Activo de Información crítico:** activos de información que permiten mantener y asegurar la correcta operación de los servicios que forman parte del núcleo de Negocio de la Corporación.
- **Incidente de Seguridad Informática:** una amenaza o violación que comprometen la seguridad de un sistema en su confidencialidad, integridad o disponibilidad.
- **Incidente de Seguridad de la información:** es indicado por un único o una serie de eventos indeseados o inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información.
- **Evento de seguridad informática:** es una ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, la falla de medidas de seguridad o una situación previamente desconocida, que pueda ser relevante para la seguridad**.**
- **Mesa de Servicios:** Centro de atención y soporte a usuarios TIC. Se conocerá como Mesa de Servicios indistintamente a los centros de atención de las unidades de negocio o al Corporativo cuando sea implementado.

Sección IX

Guía de adquisición, desarrollo y mantenimiento de sistemas de información

SIC-GMS-001-2014

Revisión 2

Febrero - 2015

CONTENIDO

INTRODUCCIÓN

Definir procesos y formatos que permitan contar con controles para la adquisición, desarrollo y mantenimiento Sistemas Informáticos en la Corporación, cuyo propósito es establecer los criterios que deben cumplir los procesos de adquisición, desarrollo y mantenimiento de los sistemas de información en la Corporación, de forma de garantizar que la seguridad de la información sea parte integral de todos los sistemas.

En los procesos de adquisición, desarrollo o mantenimiento de software se considerarán: estándares de desarrollo, de documentación y de calidad, el diseño lógico y físico de las aplicaciones, la inclusión apropiada de controles de aplicación diseñados para prevenir, detectar y corregir errores e irregularidades de procesamiento, de modo que éste sea exacto, completo, oportuno, aprobado y auditable.

La presente guía, ha tomado como marco referencia la norma técnica internacional ISO27002:2013 en el ítem “14. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información”, la Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27002:2009 en el ítem “12. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información”.

En la presente Guía se verifican temas referentes al análisis y especificaciones de los requerimientos de seguridad que deben ser identificados en todas las fases de los sistemas de información.

ALCANCE

La presente Guía aplica a todos los sistemas de información de la Corporación, incluyendo los técnicos como SCADA, RAP, GIS, entre otros, y que se encuentren en cualquier oficina, centro de datos, subestación o localidad de la Corporación.

Información referencial sobre los criterios para los productos de la seguridad de la tecnología de la información se puede encontrar en la norma ISO/IEC15408 o en otras normas sobre evaluación y certificación, según sea al caso.

OBJETIVO

- Definir, identificar y evaluar las especificaciones y requerimientos de seguridad, de acuerdo a solicitudes funcionales y técnicas.
- Establecer controles para el desarrollo o compra del software de aplicación, así como el tratamiento que se dará a aquellos procesos de emergencia que pudieran presentarse.

1 REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

a) Todos los requerimientos de seguridad deben ser identificados en las fases de análisis y especificación de requerimientos de cada proyecto, por el Gerente del proyecto con el apoyo del Equipo de Seguridad.
b) Lo anterior debe ser documentado como parte del proceso global para un sistema de información, en lo posible previo a la fase de desarrollo, implementación o contratación. Esta documentación la debe realizar el Gerente del proyecto.

1.1 Análisis y especificación de requerimientos de seguridad

El personal a cargo de la implementación de un sistema de información, con el apoyo del Equipo de Seguridad de Información deberá:

a) Evaluar los requerimientos de seguridad y los controles requeridos, proporcionales en costo y esfuerzo al valor del activo de información, que se quiere proteger y el daño potencial que pudiera ocasionar a las actividades realizadas por falla o falta de seguridad.
b) Definir los controles de seguridad de información apropiados para el mantenimiento y desarrollo de sistemas, tanto automatizados como manuales. En esta definición deben participar personal del requerimiento funcional y personal técnico que trabajarán en el sistema.
c) Para los procesos de gestión de riesgos para identificar los requisitos de los controles de la seguridad, se podría tomar como referencia la norma ISO/IEC TR 13335-3.

2 PROCESAMIENTO CORRECTO DE LAS APLICACIONES

a) El área de TIC, deberá definir, mantener y aplicar un estándar Corporativo para: codificación de software, nomenclaturas, interfaz de usuario, interoperabilidad, eficiencia de desempeño de sistemas, escalabilidad, validación contra requerimientos, planes de pruebas unitarias y de integración.
b) Las áreas de TIC o los responsables de la administración de los sistemas técnicos deberán garantizar que exista diagramas, manuales técnicos, de instalación y configuración; así como de usuario, los cuales serán difundidos a quien fuere estrictamente necesario; y, actualizados de forma permanente.

2.1 Control del procesamiento interno

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá asegurase que:

a) Las especificaciones del diseño de la arquitectura tecnológica y de información definidas dentro de la organización, consideren mecanismos de autorización, integridad de la información, control de acceso, respaldos, diseño e implementación de pistas de auditoría y requerimientos de seguridad.
b) La implementación de software aplicativo adquirido incluya los procedimientos de configuración, aceptación y prueba personalizados e implantados.
c) Exista eficiencia en el desempeño del sistema, la documentación y los manuales de usuario, integración y planes de prueba del sistema.
d) Se implemente los aspectos técnicos necesarios para la validación de la arquitectura de información de la organización, las aplicaciones existentes, la interoperabilidad con las aplicaciones existentes y los sistemas de bases de datos, dentro del control de procesamiento.

2.2 Adquisición de productos, programas de computación

Todos los Servidores a cargo de una adquisición de productos informáticos, sistemas de información o programas de computación, con el apoyo de las áreas de TIC, Centros de Control y Equipo de seguridad deberán:

a) Identificar, priorizar, especificar y llegar a un acuerdo sobre los

requerimientos funcionales y técnicos con la participación y aprobación formal de los usuarios, donde se incluirá tipos de usuarios, requerimientos entrada, definición de interfaces, archivo, procesamiento, salida, control, plan de pruebas y trazabilidad o pistas de auditoría de las transacciones en donde aplique.

b) Especificar criterios de aceptación de los requerimientos que cubrirán la definición de las necesidades, su factibilidad tecnológica y económica, el análisis de riesgo y de costo-beneficio, la estrategia de desarrollo o compra del software de aplicación.
c) Especificar y documentar el tratamiento que se dará a aquellos procesos de emergencia que pudieran presentarse
d) Establecer los requisitos de seguridad que el producto debe contemplar.
e) La adquisición de software o soluciones tecnológicas se realizará sobre la base del portafolio de proyectos y servicios priorizados en los planes estratégico y operativo previamente aprobados. Para adquisiciones que no consten en los planes mencionados, se deberá solicitar autorización previa de la máxima autoridad de la Corporación.
f) Los contratos tendrán el suficiente nivel de detalle en los aspectos técnicos relacionados, garantizar la obtención de las licencias de uso y/o servicios, definir los procedimientos para la recepción de productos y documentación en general, además de puntualizar la garantía formal de soporte, mantenimiento y actualización ofrecida por el proveedor.
g) Es necesario formalizar con actas de aceptación por parte de los usuarios, el paso de los sistemas probados y aprobados desde el ambiente de desarrollo/prueba al de producción y su revisión en la post-implantación.

3 CONTROLES CRIPTOGRÁFICOS

Como parte de la adquisición, desarrollo o mantenimiento de sistemas el área de TIC y/o Administradores de Sistemas de Centros de Operación y Control, con el apoyo del Equipo de Seguridad de Información, deberán tomar en cuenta los controles criptográficos. Para ello deberán asegurase que:

a) Se garantice:
    - Confidencialidad: uso de cifrado (encriptación) de la información para proteger información sensible o crítica, bien sea almacenada o transmitida
    - Integridad / autenticidad: uso de firmas electrónicas o códigos de autenticación de mensajes para proteger la autenticidad e

integridad de información sensible o crítica transmitida o almacenada
- No-repudio: uso de técnicas de cifrado (criptográficas) para obtener prueba de la ocurrencia o no ocurrencia de un evento o acción.

b) Se haga uso de controles de cifrado (criptográficos) para la protección de la información sensible transportada por medios móviles o removibles, por dispositivos especiales, o a través de los medios de comunicación.
c) Se definan los algoritmos de cifrado (encriptación) que se utilizarán en toda la Corporación, dependiendo del tipo de control a aplicar, el propósito y el proceso del negocio. Esta definición debe ser periódicamente revisada y actualizada.
d) Se identifique el nivel requerido de protección de datos que se almacenará en el sistema, considerando: el tipo, fortaleza y calidad del algoritmo de cifrado (encriptación) requerido.

3.1 Política de uso de los controles criptográfico

Los responsables del área de TIC y/o Administradores de Sistemas de Centros de Operación y Control se encargarán de:

a) Implementar la Política de Controles
b) Administrar las claves: gestión de claves, incluyendo su generación

Los Operadores de Seguridad deberán:

c) Definir las normas de controles de cifrado (criptográficos) que se adoptarán, para la implementación eficaz en toda la Corporación; establecer la solución a usar para cada proceso del negocio que sea necesario.
d) Desarrollar procedimientos de administración de claves, de recuperación de información cifrada en caso de pérdida, de compromiso o daño de las claves y de reemplazo de claves de cifrado.

El Oficial de Seguridad de Información, en conjunto con el Equipo de Seguridad de Información, se encargará de:

e) Proponer las normas y procedimientos necesarios para:
    i. generar claves para diferentes sistemas criptográficos y diferentes aplicaciones, incluyendo fechas de inicio y caducidad de vigencia de las claves;

ii. generar y obtener certificados de clave pública de manera segura;
iii. distribuir las claves públicas de forma segura a los usuarios, incluyendo información sobre cómo deben activarse cuándo se reciban las mismas;
iv. almacenar claves, incluyendo la forma de acceso a las mismas, por parte de los usuarios autorizados;
v. cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las claves;
vi. revocar claves, incluyendo cómo deben retirarse o desactivarse las mismas;
vii. archivar claves; por ejemplo, para la información archivada o resguardada;
viii. registrar y auditar las actividades relativas a la administración de claves.

3.2 Controles criptográficos básicos

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Utilizar controles criptográficos para la protección de claves de acceso a: sistemas, datos y servicios. Las claves deberán ser almacenadas de manera codificada, cifrada (encriptado) en la base de datos y/o en archivos de parámetros.
b) Utilizar controles de cifrado (criptográficos) para la transmisión de información Confidencial, fuera del ámbito de la Corporación.
c) Uso de firma electrónica:
   - Utilizar certificados electrónicos de Entidad de Certificación de Información reconocidas por el Estado Ecuatoriano para la firma de cualquier tipo de documento, mensaje de dato, transacción que se procese electrónicamente o para comunicaciones entre sistemas, aplicaciones y medios físicos.
   - Utilizar los certificados electrónicos emitidos bajo estándares por las Entidades de Certificación de Información, las cuales deben ser instituciones u organizaciones reconocidas, con controles y procedimientos idóneos establecidos para proporcionar el grado requerido de confianza.
   - Utilizar los certificados electrónicos según el ámbito para la cual fue generado.

3.3 Protección de claves cifradas (criptográficas)

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control, en coordinación con el Equipo de Seguridad de Información deberán:

a) Implementar un sistema de administración (generación, almacenamiento, respaldo y eliminación segura) de claves cifradas (criptográficas). Este sistema deberá permitir trabajar como mínimo con dos tipos de técnicas criptográficas: técnicas de clave secreta (criptografía simétrica) y técnicas de clave pública (criptografía asimétrica). Este sistema deberá además:
    - Incorporar funcionalidad para cambiar o actualizar las claves, incluyendo reglas sobre cuándo cambiarlas, cómo hacerlo y la forma en que los usuarios autorizados tendrán acceso a ellas.
    - Incorporar funcionalidad para tratar las claves perdidas. Bajo pedido del usuario que pierde una clave se generará una nueva, la entrega será a través del procedimiento definido para la entrega de la primera clave.
    - Permitir revocar las claves, incluyendo la forma de retirarlas o desactivarlas cuando las claves se han puesto en peligro o cuando un usuario se retira de la Corporación.
    - Incorporar funcionalidad para recuperar claves perdidas o corruptas como parte de la gestión de continuidad de los servicios informáticos.
b) Proteger todas las claves contra modificación y destrucción.
c) Proteger las claves secretas y privadas contra copia o divulgación no autorizada.
d) Proporcionar una protección adecuada al equipamiento que permite generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.
e) Habilitar en los sistemas, la generación de claves temporales al momento de la creación de usuarios.
f) Distribuir la primera clave a los usuarios, incluyendo la forma de activar y confirmar la recepción de la clave. Luego, a través de un correo electrónico recibirá un acceso al sistema, el cual validará la entrega de la clave y la obligatoriedad de cambiar dicha clave.
g) Permitir archivar claves para información archivada o con copia de respaldo.
h) Registrar y auditar las actividades relacionadas con la gestión de claves.

4 SEGURIDAD DE LOS ARCHIVOS DE SISTEMA

4.1 Control del software operativo

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

b) Definir y aplicar procesos de control de cambios para la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.
c) Definir protocolos de pruebas previo a un paso a producción para cada sistema.
d) Definir el proceso de paso a producción para cada sistema.
e) No permitir que ningún programador o analista de desarrollo y mantenimiento de aplicaciones acceda a los ambientes de producción.
f) Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones para el paso a producción, el informe de pruebas previas y el informe de paso a producción.
g) Asignar un responsable de la implantación de cambios por sistema (no podrá ser personal que pertenezca al área de desarrollo o mantenimiento), quien tendrá como funciones principales:
   - Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.
   - Asegurar que los aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.
   - Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del responsable del área encargada del testeo y del usuario final.
   - Rechazar la implementación en caso de encontrar defectos
h) Disponer del informe de paso a producción, el cual contendrá información de todos los cambios a realizar y el plan de contingencia.
i) Guardar o instalar únicamente los ejecutables y cualquier elemento necesario para la ejecución de un software en el ambiente de producción.
j) Implementar el ensayo en el ambiente de pruebas[13]. Este ambiente debe ser similar al ambiente de producción, incluyendo los datos que puedan ser copiados. El ensayo será en base al informe de paso a producción. Se ejecutarán todas las acciones definidas y se realizarán

[13] El ambiente de pruebas puede ser llamado también ambiente de implementación como lo dicta la Norma Técnica de Seguridad de Información.

pruebas sobre capacidad de uso, seguridad, efectos en otros sistemas y facilidad para el usuario.

k) Llevar un registro de auditoría de las actualizaciones realizadas.
l) Retener las versiones previas del sistema, como medida de contingencia.
m) Denegar permisos de modificación a los desarrolladores, sobre los programas fuentes bajo su custodia.
n) Usar un sistema de control de configuración para mantener el control del software instalado, así como de la documentación del sistema.
o) Entregar acceso físico o lógico al ambiente producción únicamente para propósitos de soporte, cuando sea necesario y con aprobación del responsable del área de Tecnologías de la Información y Comunicaciones, esto se realizará tanto para usuarios internos de la dirección como para proveedores.
p) Monitorear las actividades de soporte realizadas sobre el ambiente de producción.
q) Registrar la copia y la utilización de la información para futuras auditorías.
r) Se considerarán como excepciones, los casos en que se requiera realizar modificaciones directamente sobre la base de datos. El Oficial de Seguridad de la Información definirá los procedimientos para la gestión de dichas excepciones que contemplarán lo siguiente:
    - Se generará una solicitud formal para la realización de la modificación o actualización del dato. No se aceptará eliminación de datos bajo ninguna circunstancia.
    - El Propietario de la Información afectada y el Oficial de Seguridad de la Información aprobarán la ejecución del cambio evaluando las razones por las cuales se solicita.
    - Se generarán cuentas de usuario de emergencia para ser utilizadas en la ejecución de excepciones. Las mismas serán protegidas mediante contraseñas, la cuales estarán sujetas al procedimiento de administración de contraseñas críticas y habilitadas sólo ante un requerimiento de emergencia y por el lapso que ésta dure.
    - Se designará un encargado de implementar los cambios, el cual no será personal del área de Desarrollo. En el caso de que esta función no pueda ser separada del área de Desarrollo, se aplicarán controles adicionales de acuerdo a la separación de funciones.
    - Se registrarán todas las actividades realizadas con las cuentas de emergencia. Dicho registro será revisado posteriormente por el Oficial de Seguridad.

Para todo lo antes mencionado, se deberá formalizar cada actividad mediante

un documento oficial.

4.2 Protección de los datos de pruebas del sistema

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Identificar por cada sistema, los datos que pueden ser copiados de un ambiente de producción a un ambiente de pruebas.
b) Efectuar pruebas de los sistemas en el ambiente de pruebas, sobre datos extraídos del ambiente de producción.
c) Solicitar autorización formal para realizar una copia de la base de datos de producción como base de datos de prueba.
d) Personalizar los datos en el ambiente de pruebas, eliminando las contraseñas de producción y generando nuevas para pruebas.
e) Identificar los datos críticos que deberán ser modificados o eliminados del ambiente de pruebas.
f) Aplicar los mismos procedimientos de control de acceso que existen en la base de producción.
g) Eliminar inmediatamente, una vez completadas las pruebas, la información de producción utilizada.

4.3 Control de acceso al código fuente disponible de los programas

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Asignar a un Administrador de programas fuentes, quien tendrá en custodia los mismos y deberá cumplir con determinadas actividades, relacionadas al acceso:
    - Utilizar un manejador de versiones para los código fuentes, proporcionar permisos de acceso a los desarrolladores bajo autorizaciones.
    - Proveer al área de Desarrollo los programas fuentes solicitados para su modificación, manteniendo en todo momento la correlación programa fuente/ejecutable.
    - Llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, programador, autorizador, versión, fecha de última modificación y fecha/hora de compilación y estado (en modificación o en producción).
    - Verificar que el autorizador de la solicitud de un programa fuente

sea el designado para la aplicación, rechazando el pedido en caso contrario.
- Registrar cada solicitud aprobada.
- Asegurar que un mismo programa fuente no sea modificado simultáneamente por más de un desarrollador, sin un manejador de versiones.

b) Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen.
c) Establecer que el responsable de implantación en producción efectuará la generación del programa objeto o ejecutable que estará en producción (compilación), a fin de garantizar tal correspondencia.
d) Desarrollar un procedimiento que garantice que cuando se migre a producción el módulo fuente, de preferencia se cree el código ejecutable correspondiente de forma automática.
e) Evitar que la función de Administrador de programas fuentes, sea ejercida por personal que pertenezca al área de desarrollo y/o mantenimiento.
f) Prohibir el almacenamiento de programas fuentes de sistemas que no están en producción, excepto en la ubicación y medio autorizado por el Oficial de Seguridad de Información.
g) Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuentes.
h) Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos como respaldos de información.
i) No mantener las bibliotecas fuente de programas en los sistemas operativos, cuando sea posible.
j) Administrar el código fuente y las bibliotecas fuente de programas de acuerdo con los procedimientos establecidos.
k) Efectuar la actualización del código fuente de programas y de los elementos asociados, así como la emisión de fuentes de programa a los programadores, solamente después de recibir la autorización apropiada.
l) Conservar un registro para auditoría de todos los accesos al código fuente de programas.
m) El mantenimiento y el copiado del código fuente de programas deberán estar sujetos a un procedimiento estricto de control de cambios.
n) Verificar que el código fuente de los sistemas no contenga puertas traseras o cualquier tipo de código malicioso.

5 SEGURIDAD EN LOS PROCESOS DE CAMBIO EN DESARROLLO Y SOPORTE

5.1 Control de Cambios

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

5.1.1 Antes de ejecutar un cambio

a) Disponer de la autorización del Subdirector o Jefe del área de Tecnologías de la Información y Comunicaciones que apruebe el cambio.
b) Analizar los términos y condiciones de la licencia, si es del caso, a fin de determinar si las modificaciones se encuentran autorizadas.
c) Determinar la conveniencia de que la modificación sea efectuada por la Corporación, por el proveedor o por un tercero, y evaluar el impacto.
d) Crear una comisión de Control de Cambios para cada cambio en el sistema.
e) Verificar que los cambios sean propuestos por usuarios autorizados y se respete los términos y condiciones que surjan de la licencia de uso, en caso de existir.
f) Elaborar el informe de paso de pruebas a producción, que deberá contener el detalle de los cambios y acciones a ejecutar, tanto de software, bases de datos y hardware:
    - Archivos a modificar;
    - Script de base de datos a ejecutar en la secuencia correcta de ejecución;
    - Script de inicialización de datos;
    - Creación de directorios;
    - Script de creación de tareas periódicas, en caso de ser necesario;
    - Plan de contingencia;
    - Protocolo de pruebas de verificación el cambio a los servicios o sistemas que afecta;
    - Mantener un registro de los niveles de autorización acordados;
    - Definir el punto de no retorno;
    - Definir las condiciones para determinar la restauración al estado anterior.
g) Obtener aprobación formal del cronograma de implementación del cambio, por parte del responsable del área de Tecnologías de la

Información.

h) Garantizar que los cambios sean informados con anterioridad a la implementación.

5.1.2 Durante la implementación de cambios

a) Implementar funcionalidades para que se pueda solicitar la autorización del propietario de la información (ej., información personal), cuando se hagan cambios a sistemas donde dicha información sea procesada.
b) Notificar a los usuarios del sistema sobre el cambio a realizar. Se enviará una notificación para informar sobre el tiempo que durará la ejecución del cambio y para informar cuando se haya terminado la ejecución del cambio.
c) Abrir ventanas (espacio de tiempo) de mantenimiento con una duración definida, en la cual se contemple las acciones del cambio, pruebas y configuraciones.
d) Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios.
e) Solicitar la revisión del Equipo de Seguridad de la Información para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.
f) Obtener el aval del propietario de la información sobre los resultados de las pruebas mediante realizadas en el ambiente correspondiente.

5.1.3 Después de la puesta en producción de los cambios

a) Actualizar la documentación para cada cambio implementado, tanto en los manuales de usuario como en la documentación operativa.
b) Mantener un control de versiones para todas las actualizaciones de software.
c) Garantizar que la implementación se llevará a cabo sin alterar los procesos involucrados.
d) Definir si los cambios a realizar tienen impacto sobre la continuidad del servicio. Si un cambio implica mucha funcionalidad o impacto al software base o infraestructura, se deberá realizar un análisis a fondo sobre las afectaciones, para que se apruebe con un plan de contingencia y se identifiquen los riesgos posibles.

5.2 Revisión técnica de las aplicaciones después de los cambios.

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

a) Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.
b) Probar que los cambios realizados retornen la funcionalidad esperada.
c) Realizar las pruebas inmediatamente después de realizar el cambio y durante la ventana de mantenimiento (espacio de tiempo) definida para el cambio.
d) Disponer de un lineamiento de pruebas a realizar.
e) Entregar un informe de las pruebas realizadas.
f) Identificar si existen problemas con los cambios, para aplicar el plan de contingencia o realizar el retorno al estado anterior al cambio.

5.3 Restricciones a los cambios en los paquetes de software.

El área de TIC y/o Administradores de Sistemas de Centros de Operación y Control deberá:

b) Mantener el software original, realizando los cambios sobre una copia perfectamente identificada, la misma que deberá ser documentada.
c) Definir un proceso de gestión de las actualizaciones del software que asegure que los parches y actualizaciones aprobados, se encuentre instalados en el software autorizado.
d) Probar y documentar en su totalidad todos los cambios, de manera que se puedan volver a aplicar, si es necesario, para mejoras futuras del software.

GLOSARIO DE TÉRMINOS

- **Criptología:** Disciplina científica que se dedica al estudio de la escritura secreta.
- **Criptografía:** Ámbito de la Criptología que se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones de los mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.
- **Encriptación o Encripción:** Proceso mediante el cual se vuelve legible información considerada importante.
- **Puerta trasera:** Secuencia especial de programación dentro del código fuente de un sistema de información, mediante el cual se pueden evitar los algoritmos de seguridad para acceder al sistema.
- **Requerimientos de seguridad**: Requisitos que deben cumplir los sistemas considerando las propiedades de seguridad de información: confidencialidad, integridad, disponibilidad, no repudio y trazabilidad.