TABLA DE CONTENIDO

1 PROPÓSITO

El presente documento es una guía para orientar y facilitar la implementación de los controles de seguridad de la información en el ICE según el estándar ISO/IEC 27001 Anexo A en su versión vigente y el estándar ISA/IEC 65443 en la parte específica para OT, para tal efecto se aporta un listado de los documentos normativos en los que se pueden apoyar para consultar y ejecutar las acciones requeridas para la dependencia o negocio interesado; respecto de los cuales además es importante verificar la versión que se está utilizando al momento de gestionar los controles, así como complementarlos con buenas prácticas y estándares internacionales.

Estos lineamientos se fundamentan en la Ley General de Control Interno, en lo dispuesto en las Normas de Control Interno para el Sector Público, emitidas por la Contraloría General de la República, así como la normativa aplicable para cada control establecido.

2 ALCANCE

El presente documento es de acatamiento para todos los funcionarios y trabajadores del ICE quienes, en el alcance de sus funciones y responsabilidades, deban aplicar los principios básicos seguridad de la información y de ciberseguridad.

En caso de que se promueva la contratación de servicios con incidencia en materia de seguridad de la información, deberá incluirse en el pliego de condiciones o en el contrato la obligación de los proveedores o socios comerciales, de rendir una declaración jurada en la que se comprometen a acatar la normativa interna en materia de seguridad de la información, los presentes lineamientos, y los documentos normativos que se emitan, en la que se comprometen a mantenerse actualizados de todas las modificaciones o reformas de las disposiciones o documentos normativos en la materia, así como la obligación de concientizar, educar y formar a su personal en materia de seguridad de la información .

3 RESPONSABILIDADES

3.1 Presidencia Ejecutiva, Gerencias ICE, Divisiones y Direcciones

a) Apoyar administrativamente mediante la aprobación de recursos humanos y tecnológicos la implementación de los lineamientos y la normativa asociada.
b) Facilitar las condiciones administrativas, técnicas y físicas razonables, para lograr la exitosa implementación de estos lineamientos, con el fin de proteger la información empresarial, en coordinación con la Dirección Ciberseguridad.
c) Difundir y cumplir con lo establecido en este documento.

3.2 Gerencia General

a) Aprobar el presente documento.

3.3 Gerencia Tecnología y Soluciones Digitales

a) Revisar periódicamente este documento y recomendar las actualizaciones que correspondan.

b) Ejecutar, en coordinación con las Gerencias del ICE, las directrices estratégicas, la normativa y cualquier otra medida necesaria para la gestión de seguridad de la información, conforme al principio de eficiencia y en consideración del logro de los objetivos institucionales.

3.4 Dirección Ciberseguridad

a) Dar seguimiento a las medidas de seguridad administrativas, técnicas y físicas que estén puestas en práctica a fin de determinar su confiabilidad.

b) Identificar, monitorear y reportar cualquier observación o sospecha de debilidades en la seguridad de la información de los sistemas y ciberseguridad, servicios o productos.

c) Recibir e investigar las denuncias sobre eventuales violaciones al deber de confidencialidad por parte de los funcionarios o trabajadores que acceden, usen o procesen información confidencial, informar sobre éstas al titular subordinado del funcionario o trabajador, para lo que corresponda y solicitar un informe de lo actuado.

d) Revisar periódicamente los lineamientos establecidos, proponer los cambios que se consideren convenientes y velar por su cumplimiento.

e) Proponer en conjunto con las dependencias involucradas, los controles adecuados sobre los activos de información con el fin de lograr el cumplimiento de los lineamientos definidos en este documento.

f) Velar por el desarrollo, implementación y mejora de la normativa de seguridad de la información con el fin de garantizar la confidencialidad, integridad y disponibilidad.

g) Coordinar con la División Jurídica los mecanismos jurídicos que se consideren pertinentes para salvaguardar la información de la Institución.

h) Ejecutar y gestionar las actividades relacionadas con la seguridad de la información, en concordancia con los planes de trabajo establecidos en la Institución.

3.5 Funcionarios y trabajadores del ICE

a) Los funcionarios, y trabajadores, en el alcance de sus responsabilidades, deben conocer y acatar los lineamientos de seguridad de la información vigentes de la institución, ya que su desconocimiento no exime su cumplimiento ni la responsabilidad ante cualquier eventualidad que comprometa la seguridad de la información de la institución.

b) Contribuir a generar una cultura de protección de la información trasegada por medio de las redes.

c) Tomar todas las precauciones para proteger la información empresarial que reciba o remita debido a su trabajo.

3.6 Clientes, proveedores y socios comerciales del ICE

En toda contratación de servicios con incidencia en materia de seguridad de la información, deberá incluirse en el pliego de condiciones o el contrato la obligación de rendir una declaración jurada en la que se comprometen a acatar la normativa interna en materia de seguridad de la información, entre ellos los presentes lineamientos, los controles establecidos, y los documentos normativos que se emitan, la obligación de mantenerse actualizados de todas las modificaciones o reformas de las disposiciones o documentos normativos en la materia, así como, cuando corresponda, la obligación de las empresas de concientizar, educar, capacitar y formar al personal en materia de seguridad de la información.

4 TÉRMINOS Y DEFINICIONES

Actividad sospechosa: Cualquier evento anómalo, que no está identificado dentro del comportamiento usual de la institución.

Activo: Se refiere a un recurso controlado por la institución y del cual se espera que soporte los objetivos de dicha organización, el recurso puede ser insumo o producto de los diferentes procesos que componen los sistemas de la entidad.

Activos críticos: Aquellos recursos que en su ausencia o falta de disponibilidad podrían degradar la habilidad de la institución para cumplir con su misión. También se consideran activos críticos a aquellos recursos que el tiempo en que la institución pueda funcionar sin ellos sea menor que el tiempo necesario para reemplazarlo.

Activos de información: Recurso de información que tiene valor para la empresa.

ADSL: (Asimetric Digital Subscriber Line o Línea de Abonado Digital Asimétrica) Es una tecnología de módem que transforma las líneas telefónicas o el par de cobre del

abonado en líneas de alta velocidad permanentemente establecidas, con el pago de una única cantidad mensual.

Análisis de vulnerabilidades: Análisis y detección de vulnerabilidades en equipos de cómputo, mediante herramientas y script automatizados. Para identificar su nivel de riesgo y visibilidad ante amenazas y ataques informáticos.

Api: Son mecanismos que permiten a dos componentes de software comunicarse entre sí mediante un conjunto de definiciones y protocolos.

Arquitectura empresarial de seguridad de la información: Esquema de acción estratégico en la institución, mediante el cual se provee a la empresa de los mecanismos que permiten traducir los requerimientos de seguridad de la información empresarial, junto con principios generales y mejores prácticas, en soluciones de seguridad de la información operacional y gestión de riesgo específicas.

Autenticación: capacidad de demostrar que un usuario o una aplicación es realmente quién dicha persona o aplicación asegura ser. Según ISO/IEC 27000, es provisión de garantía de que una característica solicitada de una entidad es correcta.

Autorización: protege los recursos importantes de un sistema, ya que limita el acceso solamente a los usuarios autorizados y a sus aplicaciones. Impide que los recursos se utilicen sin la autorización necesaria.

BIA: (Bussiness Impact Analysis) Es un análisis de impacto al negocio mediante un proceso sistemático para determinar y evaluar los efectos potenciales de una interrupción de las operaciones comerciales críticas como resultado de un desastre, accidente o emergencia.

BYOD: (Bring Your Own Device), del inglés trae tu propio dispositivo, es la política empresarial que consiste en que los funcionarios o trabajadores utilicen sus dispositivos personales para acceder a recursos de la empresa, como puede ser el correo electrónico, bases de datos o aplicaciones personales.

CAPTCHA: (Completely Automated Public Turing test to tell Computers and Humans Apart) Es una prueba de público y automático para distinguir a los ordenadores de los humanos) es un tipo de medida de seguridad conocido como autenticación pregunta-respuesta.

CCTV: (Closed Circuit Television), Circuito cerrado de televisión es un sistema de vigilancia por medio de video para fines de control de actividades, supervisión de dependencias, personal, controles de seguridad.

CD: (Compact Disc) Disco compacto**.**

Checklist: Lista de comprobación previamente seleccionada.

CIA: Confidencialidad, Integridad y Disponibilidad (traducción del inglés).

Ciberseguridad: Es la práctica de proteger sistemas, redes y programas de ataques digitales. Por lo general, los ciberataques apuntan a acceder, modificar o destruir la información confidencial; extorsionar a los usuarios o los usuarios o interrumpir la continuidad del negocio.

Cloud: Es un término que se utiliza para describir una red mundial de servidores, cada uno con una función única. La nube no es una entidad física, sino una red enorme de servidores remotos de todo el mundo que están conectados para funcionar como un único ecosistema.

Código Fuente: Es un archivo o conjunto de archivos, que contienen instrucciones concretas, escritas en un lenguaje de programación, que posteriormente compilan uno o varios programas.

Confidencialidad: Cualidad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. (ISO/IEC 13335-1:2004).

Contraseñas hasheadas: Es típico que las contraseñas de usuario no se guarden "sin más" (es decir, en texto plano) en la base de datos, pues si esta base de datos se viera comprometida (alguien pudiera leer la información que hay en ella) tendría inmediatamente acceso a todas las contraseñas.

Criptografía: Es el desarrollo de un conjunto de técnicas que permiten alterar y modificar mensajes o archivos con el objetivo de que no puedan ser leídos por todos aquellos usuarios que no estén autorizados a hacerlo.

CSIRT: (Computer Security Incident Response Team), También conocido en español como equipo de respuesta a incidentes de seguridad informáticos, es el equipo encargado de recibir, comprobar y responder a incidentes que se detecten en su área de actuación.

Custodio de la información: Persona física o jurídica que, en el ejercicio de un rol asignado por el ICE, tiene la responsabilidad de custodiar la información de acuerdo con lo indicado por el responsable, rigiéndose por las leyes relacionadas y la normativa vigente.

CVSS: (Common Vulnerability Scoring System); en español, sistema de puntuación de vulnerabilidad común, es un estándar cuya finalidad es cuantificar la gravedad y estimar el impacto que presentan las vulnerabilidades respecto a la seguridad de un sistema.

Dato: Son representaciones simbólicas (vale decir: numéricas, alfabéticas, algorítmicas, etc.) de un determinado atributo o variable cualitativa o cuantitativa, o sea: la descripción codificada de un hecho empírico, un suceso, una entidad.

Disponibilidad: Cualidad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. (ISO/IEC 13335-1:2004).

DMZ: (Demilitarized Zone); en español, zona desmilitarizada. Consiste en una red aislada que se encuentra dentro de la red interna de la institución. En ella se encuentran ubicados exclusivamente todos los recursos de la empresa que deben ser accesibles desde Internet, como el servidor web o de correo. Por lo general, una DMZ permite las conexiones procedentes tanto de Internet como de la red local de la empresa, donde están los equipos de los trabajadores, pero las conexiones que van desde la DMZ a la red local no están permitidas. Esto se debe a que los servidores que son accesibles desde Internet son más susceptibles a sufrir un ataque que pueda comprometer su seguridad.

DR: La recuperación ante desastres (DR) es la capacidad de una organización para responder y recuperarse de un evento que afecta negativamente a las operaciones comerciales. El objetivo de los métodos de DR es permitir que la institución recupere el uso de sistemas críticos e infraestructura de TI tan pronto como sea posible después de que ocurra un desastre.

DRP: (Disaster Recovery Plan); El Plan de Recuperación de Desastres es un documento que enumera todos los procesos que la institución debe implementar para mantener o reconstruir su infraestructura de TI después de una crisis cibernética. Indica cómo y cuándo diferir al sistema de respaldo, como se detalla en el plan de gestión de crisis, y especifica qué sistema de respaldo activar para garantizar la seguridad de los datos confidenciales.

Dueño de la información: Persona física o jurídica que tiene poder de usar y disponer de la información según la normativa relacionada (ICE, clientes, socios del negocio, funcionarios, trabajadores).

DVD: Acrónimo en inglés de *Digital Versatile Disc* (Disco Versátil Digital) es un tipo de disco óptico para almacenamiento de datos.

Electromecánica: Es la combinación de las ciencias del electromagnetismo de la ingeniería eléctrica y la ciencia de la mecánica. La Ingeniería Electromecánica es la disciplina académica que la aborda, gracias a ella se han producido importantes avances en el desarrollo tecnológico en la mayoría de los campos científicos.

Enmascaramiento de datos: Es el proceso mediante el cual se cambian ciertos elementos de los datos de un almacén de datos, cambiando su información, pero

consiguiendo que la estructura permanezca similar, de forma que la información sensible quede protegida. El enmascaramiento de datos garantiza que la información sensible del cliente no está disponible fuera del entorno de producción. Se trata de una técnica especialmente en situaciones como la formación de usuarios o pruebas de software.

Endpoint: Un punto final es cualquier dispositivo físico que se puede conectar a una red, incluidas computadoras, computadoras portátiles, teléfonos móviles, tabletas y servidores. La lista de puntos finales continúa creciendo para incluir muchos elementos no tradicionales, como impresoras, cámaras, electrodomésticos, relojes inteligentes, rastreadores de salud, sistemas de navegación y cualquier otro dispositivo que se pueda conectar a Internet.

Entidad: Una entidad es una cosa u objeto. del mundo real, también puede ser un concepto abstracto y es distinguible de todos los demás objetos. Una entidad tiene un conjunto de propiedades o atributos que la caracterizan.

Entidades no Humanas: No humana, o no-humana/o, es una expresión utilizada para describir a cualquier entidad que presente características humanas, pero no las suficientes como para ser consideradas como tales. Este término en su comprensión es muy técnico y es usado exclusivamente por personal técnico especializado.

Firewall: Es un dispositivo de seguridad de la red que monitorea el tráfico de red —entrante y saliente— y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad**.**

Front End: Es la interfaz gráfica de usuario de un equipo que facilita su uso.

GDI: Gestión Documental Institucional.

GTSD: Gerencia Tecnología y Soluciones Digitales.

Hardware: Es el conjunto de los componentes materiales, tangibles, de un computador o un sistema informático.

Hash: Tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte en un rango de salida finito, normalmente cadenas de longitud fija.

Host: Es todo el equipo informático que tiene una dirección IP y está interconectado con uno o más ordenadores. Un host o host es un equipo que funciona como punto de inicio y fin de las transferencias de datos. Descrito comúnmente como el lugar donde reside un sitio web.

IaaS: (Infrastructure as a Service); Es un servicio de computación en la nube en el que las empresas alquilan o arriendan servidores para computación y almacenamiento en la nube. Los usuarios pueden ejecutar cualquier sistema

operativo o aplicaciones en los servidores alquilados sin los costos de mantenimiento y operación de esos servidores.

ICE: Instituto Costarricense de Electricidad.

IIP: Información de Identificación Personal es **cualquier dato que podría identificar a un individuo específico**. La IIP incluye, entre otros, el nombre, el número de la Seguridad Social, la fecha de nacimiento, el domicilio y los datos biométricos.

Incidente de seguridad de la información: Evento o serie de eventos de seguridad adversos (actividades sospechosas) que ponen en riesgo la confidencialidad, integridad y disponibilidad de los datos y sistemas de información, incumpliendo con los principios establecidos en la política de seguridad de la información.

Información: Es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada. (ISO 27K)

Información empresarial: Conjunto de datos procesados que tienen un significado para la Empresa en un momento y lugar determinados (incluye adicionalmente la información suministrada por clientes y terceros), independiente de su soporte y que como activo estratégico tiene un alto valor para el ICE.

Información sensible: Información relativa a datos personales de los usuarios, clientes y de los funcionarios y trabajadores de la Institución, información declarada confidencial en los términos del artículo 35 de la ley 8660, información asociada a propiedad intelectual, información asociada a controles, estrategias y vulnerabilidades de ciberseguridad, así como cualquier otra que por disposición constitucional o legal ostente la condición de información privada o confidencial, entre otra que sea de importancia para la Institución.

INTECO: Instituto de Normas Técnicas de Costa Rica.

Integridad: Cualidad de salvaguardar la exactitud y estado completo de los activos (ISO/IEC 13335-1:2004).

Inteligencia Artificial (AI): Es la habilidad de una máquina de presentar las mismas capacidades que los seres humanos, como el razonamiento, el aprendizaje, la creatividad y la capacidad de planear.

IP: El método o protocolo por el cual se envían datos de una computadora a otra en Internet. Cada computadora conocida como host, en Internet tiene al menos una dirección IP que la identifica de manera única de todas las demás computadoras en Internet.

Internet: Es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, lo cual garantiza que las redes físicas heterogéneas que la componen constituyen una red lógica única de alcance mundial.

Intranet: Es una red informática que utiliza la tecnología del protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización. Suele ser interna, en vez de pública como internet, por lo que solo los miembros de esa organización tienen acceso a ella.

Log: Es un archivo de texto en el que constan cronológicamente los acontecimientos que han ido afectando a un sistema informático (programa, aplicación, servidor, etc.), así como el conjunto de cambios que estos han generado.

Malware: Abreviatura de Malicious Software, término que engloba todo tipo de código de computadora cuya función es dañar un sistema o causar un mal funcionamiento entre los más comunes podemos encontrar Troyanos (Trojans), Gusanos (worm), Marcadores, (dialers), Programas espías (spyware), Códigos adicionales (adware), Secuestradores (hijackers), Capturadores de teclado (keyloggers), Falsos programas de seguridad (Fake AVS o Rogues), herramientas que esconden procesos y que permiten a los intrusos acceso sistemas con fines maliciosos (rootkits, bootkits).

Merge: Es la operación que permite "mezclar" el código correspondiente a dos modificaciones simultáneas hechas en paralelo a un mismo programa.

NIST Instituto Nacional de Estándares y Tecnología del Gobierno de USA.

OWASP: (Open Web Application Security Project); Es una comunidad en línea que produce artículos, metodologías, documentación, herramientas y tecnologías disponibles gratuitamente en el campo de la seguridad de aplicaciones web. El OWASP proporciona recursos gratuitos y abiertos.

PaaS: (Platform as a Service); Es un modelo de computación en la nube que proporciona a los clientes una plataforma en la nube completa (hardware, software e infraestructura) para desarrollar, ejecutar y administrar aplicaciones sin el costo, la complejidad y la inflexibilidad que a menudo conlleva la creación y el mantenimiento de esa plataforma local.

Partes Interesadas: Para cada organización las partes interesadas pueden ser diferentes. Pero se puede decir que las partes interesadas, en una organización típica, son, entre otras:

1. Funcionarios y trabajadores.
2. Propietario, órgano de dirección y alta gerencia.
3. Agencias gubernamentales con autoridad regulatoria.

4. Clientes.
5. Proveedores.
6. Socios comerciales.

Phishing: Es un ataque informático de ingeniería social que usa medios de comunicación digitales, como el correo electrónico, para engañar y estafar a las personas. A través de técnicas de manipulación emocional genera confianza en las personas para poder robar su información y dinero.

Pin: (Personal Identification Number); El pin es un número de identificación personal que utilizan ciertos aparatos electrónicos a modo de contraseña numérica.

Proveedor: Un proveedor es una persona o un negocio que vende productos o brinda servicios con fines de lucro. Puede funcionar en un entorno de negocio a consumidor (B2C) o de negocio a negocio (B2B). En el entorno B2B, los proveedores suelen llamarse mayoristas.

RACI: La matriz RACI o matriz de responsabilidades es un instrumento de organización, el cual adopta la forma de un cuadro de asignación de recursos. En éste, se busca definir los roles y responsabilidades de los diversos actores que participan en la realización de un proyecto.

RDSI: (Red Digital de Servicios Integrados); Es una "red digital con servicios integrados". En pocas palabras, la RDSI es una norma específica que permite la transmisión digital de datos.

Red: Es un conjunto de computadoras y dispositivos conectados entre sí. La conexión se puede hacer a través de cables, normalmente Ethernet, o de forma inalámbrica. Las computadoras conectadas entre sí pueden compartir recursos como el acceso a Internet, impresoras, servidores de archivos y otros.

Redundancia: es una forma de asegurarse de que tus datos están respaldados y almacenados en múltiples lugares para ayudar a protegerlos contra pérdidas o daños. Una redundancia bien diseñada también puede ayudar a proteger contra desastres naturales y otros imprevistos.

Responsable de la información: Persona física o jurídica, que, en el ejercicio de un rol asignado por el ICE, tiene a su cargo la gestión de la información, desde su creación hasta su eliminación una vez cumplida la vigencia legal-administrativa (ciclo de vida de la información), rigiéndose por leyes relacionadas y la normativa vigente.

Riesgo: Probabilidad de que ocurran eventos que tendrían consecuencias sobre el cumplimiento de los objetivos fijados (Procedimiento para la Valoración de Riesgos y la Continuidad del Negocio (Metodología) 38.01.002.2006)

Riesgo Cibernético: Es la exposición potencial a pérdidas o daños derivados de los sistemas de información o comunicaciones de una organización. Los ataques cibernéticos, o violaciones de datos, son dos ejemplos de riesgo cibernético que se reportan con frecuencia.

Roll-Back: Es una operación que devuelve a la base de datos, algún estado previo. Las reversiones son importantes para la integridad de la base de datos, a causa de que significan que la base de datos puede ser restaurada a una copia limpia incluso después de que se han realizado operaciones erróneas. Son cruciales para la recuperación ante errores de un servidor de base de datos, como por ejemplo un cuelgue del equipo. Al realizar una reversión cualquier transacción que estuviera activa en el tiempo del cuelgue es revertida y la base de datos se ve restaurada a un estado consistente.

Root: Es el nombre convencional de la cuenta de usuario que posee todos los derechos en todos los modos (monousuario o multiusuario). Normalmente es la cuenta de administrador. El usuario Root puede hacer muchas cosas que un usuario común no puede, tales como cambiar el dueño o permisos de archivos y enlazar a puertos de numeración pequeña.

Router: Es un dispositivo que permite interconectar redes con distinto prefijo en su dirección IP. Su función es la de establecer la mejor ruta que destinará a cada paquete de datos para llegar a la red y al dispositivo de destino. Es bastante utilizado para conectarse a Internet ya que conecta la red de nuestro hogar, oficina o cualquier red a la red de nuestro proveedor de este servicio. La mayoría de los routers que se utilizan para el hogar y oficinas tienen incorporadas otras funciones adicionales al enrutador.

RTO: Expresa el tiempo durante el cual una organización pueda tolerar la falta de funcionamiento de sus aplicaciones y la caída de nivel de servicio asociada, sin afectar a la continuidad del negocio.

SAI: (Sistema de Alimentación Ininterrumpida); En inglés, UPS; uninterruptible power supply, y lo que se consigue con ello es asegurar el funcionamiento de un equipo aun cuando deja de haber suministro eléctrico.

SDN: Son un conjunto de técnicas relacionadas con el área de redes computacionales, cuyo objetivo es facilitar la implementación e implantación de servicios de red de una manera determinista, dinámica y escalable, evitando al administrador de red gestionar dichos servicios a bajo nivel. Todo esto se consigue mediante la separación del plano de control del plano de datos.1

SD-WAN: Es una red de área amplia que utiliza tecnología de red definida por software, como la comunicación a través de Internet mediante túneles superpuestos que se cifran cuando se destinan a ubicaciones internas de la institución.

Seguridad de la información: La preservación de la confidencialidad, la integridad y la disponibilidad de la información. Además, otras cualidades tales como la autenticidad, la rendición de cuentas, el no repudio y la confiabilidad también pueden ser consideradas (INTE/ISO/IEC 27000).

Servidor: Es a un computador configurado con ciertas características que le permitan manejar grandes volúmenes de información, para proveerla a otros equipos conocidos como estaciones o clientes, en el momento que la requieran, interactuando en una red.

SGSI: Sistema de Gestión de la Seguridad de la Información.

SIEM: (Security Information and Event Management); es una combinación de dos conceptos: SIM (Security Information Management) y SEM (Security Event Management). Esta unión plantea un enfoque basado en software que permite obtener una visión completa de la seguridad informática. Un sistema SIEM considera en todo momento los requisitos específicos de la empresa, siempre que existan definiciones claras e individuales sobre qué procesos y eventos son relevantes para la seguridad, así como de qué manera y con qué prioridad es preciso reaccionar ante ellos. Por esta razón, el Security Information and Event Management puede entenderse también como un conjunto exhaustivo de normas para los estándares de seguridad existentes y de directrices para mantener la calidad de las operaciones informáticas de una empresa.

SLA: (Service Level Agreement) Acuerdo o nivel de servicio.

Software: Es un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora.

Software malicioso: Es cualquier software que daña un sistema informático. El programa maligno puede tener forma de gusanos, virus, troyanos, spyware, adware y rootkits, etc., que roban datos protegidos, eliminan documentos o agregan software no aprobado por un usuario.

Spyware: Es un tipo de programa que se instala con o sin su permiso en las computadoras para recopilar información acerca de los usuarios, sus equipos o los hábitos de navegación, supervisa todas sus actividades sin su conocimiento y envía estos datos a un usuario remoto. También puede descargar otros programas maliciosos de Internet e instalarlos en su equipo. El spyware actúa como adware

(publicidad no deseada) pero suele tratarse de un programa aparte que se instala sin su conocimiento mientras se instala otro programa o aplicación gratuitos.

SSH: (Secure Shell); es un método de comunicación segura con otra computadora. La parte "segura" del nombre significa que todos los datos enviados a través de una conexión SSH son cifrado. Esto significa que si un tercero intenta interceptar la información que se transfiere, parecería codificada e ilegible. La parte "shell" del nombre significa que SSH se basa en Unix shell, que es un programa que interpreta los comandos ingresados por un usuario.

Template: Es la combinación de archivos que componen la parte visual de un website. Sin duda, forma parte fundamental de toda página web y puede resultar muy útil para realizar mejoras no sólo estéticas.

Terceros: Todo individuo que no sea funcionario o trabajador del ICE (proveedores, socios comerciales, clientes, personal de proveedores, etc.)

TI: Tecnologías de Información.

TIC: Son el conjunto de tecnologías desarrolladas en la actualidad para una información y comunicación más eficiente, las cuales han modificado tanto la forma de acceder al conocimiento como las relaciones humanas.

Token: Consiste en una contraseña temporal y aleatoria que es generada por un dispositivo específico, o por un software. Esta clave se complementa con aquella que siempre usamos al ingresar nuestros datos.

Usuario de la información: Persona física o jurídica, proceso o sistema, que, en el ejercicio de un rol asignado por el ICE, debe gestionar la información, a la cual accede de forma autorizada, de acuerdo con lo indicado por el responsable, rigiéndose por las leyes relacionadas y la normativa vigente. El nivel de acceso es designado por el responsable de la información. La información empresarial, como recurso controlado por el ICE, será valorada mediante los criterios de confidencialidad, integridad y disponibilidad con el fin de determinar los controles a establecer para su gestión y preservación.

VPN: Una red privada virtual (VPN por sus siglas en inglés) es una tecnología que permite a los usuarios enviar y recibir datos a través de redes compartidas o públicas como si sus equipos informáticos estuvieran conectados directamente a la red privada.

Vulnerabilidad: Debilidad inherente o propia de un recurso o activo en partícula. Existencia de una debilidad o falla, ya sea en el diseño, o un error de implementación

que pueda ser llevado a un evento inesperado que comprometa la seguridad de un sistema.

5 CONTROLES ORGANIZACIONALES

5.1 Políticas de seguridad de la información

La política de seguridad de la información y otra normativa relacionada deben ser definidas, aprobadas por el órgano correspondiente, publicadas, comunicadas y reconocidas por el personal de la Institución. En el caso de las partes interesadas, en específico proveedores y socios comerciales que corresponda, deberá incluirse en el pliego de condiciones o el contrato la obligación de rendir una declaración jurada en la que se comprometen a acatar la normativa interna en materia de seguridad de la información, incluida esta política, a mantenerse actualizados de todas las modificaciones o reformas de las disposiciones o documentos normativos en la materia, cuando se publiquen en el Diario Oficial La Gaceta, en caso contrario (cuando no se publique en la Gaceta), el administrador del contrato, debe comunicárselas.

El ICE tiene una Política Empresarial de Seguridad de la Información, así como otras políticas y normativas relacionadas, las cuales fueron aprobadas por los órganos competentes según el caso, además han sido publicadas, comunicadas y reconocidas por el personal de la Institución y las partes interesadas. Por último, es importante mencionar que estas políticas y normativas son revisadas a intervalos planificados principalmente si se producen cambios significativos.

Propósito

Contar con políticas que funjan como marco de acción para garantizar la idoneidad, adecuación y eficacia de las actividades diarias de la Seguridad de la Información, de acuerdo con las leyes, los requisitos del negocio, los estándares internacionales y demás regulaciones.

Orientación

La Política Empresarial de Seguridad de la Información aprobada por la Gerencia General establece el enfoque para gestionar la seguridad de la información.

A un nivel subsiguiente, la Política Empresarial de Seguridad de la Información está respaldada por lineamientos específicos, que se documentan y complementan mediante este instrumento, que detalla lo que, de forma general realiza el ICE, para fortalecer la seguridad de la información.

La responsabilidad de la formulación, la revisión y de gestionar la aprobación de la normativa, políticas, y lineamientos de temas específicos en materia de seguridad de la información es coordinada por la Dirección Ciberseguridad y la Gerencia Tecnología y

Soluciones Digitales, pero participan todas las Gerencias mediante la designación formal de enlaces que facilitan dicha revisión y actualización.

Revisión de las Políticas de Seguridad de la Información

La revisión tanto de la *Política Empresarial de Seguridad de la Información del ICE,* así como de los lineamientos específicos detallados en este documento, deben incluir la evaluación de las oportunidades de mejora que surjan, como respuesta a los cambios que se produzcan tanto en el ámbito institucional como en el ámbito nacional e internacional.

Además, se tomarán en cuenta los resultados de los informes de la Auditoría Interna, así como las auditorías externas que se programen. Las revisiones exigen tomar en consideración las modificaciones que sufran las leyes, normativas, políticas o lineamientos, con el fin de lograr la coherencia y la actualización.

Se debe comunicar formalmente al personal de la institución, cada vez que se dé un cambio o actualización de la política o de cualquier otro documento normativo de seguridad de la información, y si se considera necesario, capacitar a las dependencias que así lo requieran para evacuar consultas o dudas que puedan surgir posterior a la comunicación de éstos. En el caso de las partes interesadas, tratándose de proveedores o socios comerciales, deberá incluirse en el pliego de condiciones o el contrato la obligación de rendir una declaración jurada en la que se comprometen a acatar la normativa interna en materia de seguridad de la información, a mantenerse actualizados de todas las modificaciones o reformas de las disposiciones o documentos normativos en la materia, cuando se publiquen en el Diario Oficial La Gaceta, en caso contrario (cuando no se publique en la Gaceta), el administrador del contrato, debe comunicárselas.

Si la Política Empresarial de Seguridad de la Información o cualquier lineamiento específico del tema se distribuye fuera de la institución, se debe tener cuidado de no divulgar indebidamente la información confidencial.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.

Código	Ley, Política, Norma
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

5.2 Roles y responsabilidades en materia de seguridad de la información

Los roles y responsabilidades en materia de seguridad de la información deben definirse y asignarse en función de las necesidades de la institución.

Propósito

El propósito de este control es establecer una estructura definida, aprobada y entendida para la implementación, operación, control, seguimiento y mejora de la seguridad de la información dentro de la institución.

Orientación

La asignación de funciones y las responsabilidades se realiza con base en la *Política Empresarial de Seguridad de la Información del ICE*, ahí se establecen y gestionan las responsabilidades a cumplirse para:

a) La protección de la información y otros activos asociados;
b) Llevar a cabo procesos específicos de seguridad de la información,
c) Las actividades de gestión de los riesgos de la seguridad de la información y, en particular, la aceptación de los riesgos residuales (por ejemplo, a los propietarios de los riesgos);
d) Establecer deberes y responsabilidades de todo el personal que utiliza la información y otros activos asociados.

Estas responsabilidades también son puntualizadas o detalladas según la dependencia del ICE que las aplica, por ejemplo, para los sitios o instalaciones de procesamiento de información, son dichas dependencias las que proponen los documentos normativos que les aplican, además de que tienen la responsabilidad de desarrollar sus normas, directrices, procedimientos, u otros documentos normativos que considere convenientes, las cuales serán aprobados por los órganos competentes, según las dependencias de negocio y las condiciones administrativas, técnicas u operativas donde se implementan.

A continuación, se detallan algunas de las funciones establecidas para las áreas de Seguridad de acuerdo con los estándares y que apoyan este control.

Dirección Ciberseguridad

La Dirección Ciberseguridad debe revisar y recomendar modificaciones de la normativa que se aplica en cada dependencia en particular, con el fin de que se mantenga el alineamiento con las políticas generales establecidas para la institución.

Disponer de soluciones que aseguren la protección y resguardo de los activos y de los espacios virtuales, tanto de la empresa como de los usuarios y clientes, garantizando la confiabilidad, integridad y disponibilidad de la información.

Proceso Seguridad de la Información

Definir el modelo de control, protección y propiedad de los datos, información y redes de la empresa y sus clientes, preservando la confidencialidad, disponibilidad e integridad considerando el riesgo y la auditabilidad.

Proceso Seguridad Informática

Establecer plataformas y software de seguridad para proteger la información de la organización y los clientes asegurando la continuidad del negocio.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

5.3 Segregación de funciones

Los deberes conflictivos y las dependencias de responsabilidad conflictivas deben ser segregados.

Propósito

El propósito de este control de segregación de funciones es reducir el riesgo de fraude, error y elusión de los controles de seguridad de la información y ciberseguridad.

Orientación

El ICE dentro de sus labores, regula las actividades estratégicas, tácticas y operativas en aspectos relacionados con la gobernabilidad y gestión de la seguridad de la información empresarial de acuerdo con la legislación, los reglamentos y la normativa interna vigente.

Los roles que intervienen en el tema de seguridad de la información estarán alineados a los siguientes principios indicados en el Modelo de Ciberseguridad aprobado:

a) **Oportunidad**: los funcionarios y trabajadores deberán realizar sus funciones con celeridad y de manera oportuna.
b) **Ética**: la información empresarial debe utilizarse de una forma ética, aplicando los valores de la Empresa.
c) **Participación multidisciplinaria:** las políticas, estándares, guías, procedimientos y otros mecanismos de seguridad de la información, para ser efectivos, y viables deben contemplar la participación, consideraciones y puntos de vistas de todas las dependencias de la Empresa, ya sea como gerente del negocio o responsable, custodio o usuario de la información empresarial.
d) **Transparencia:** deben existir registros que permitan evidenciar todas las acciones relacionadas con el tema de seguridad de la información.
e) **Supervisión:** para cada rol o grupo de trabajo debe haber otro rol con competencia de supervisión con la responsabilidad de comprobar y supervisar activa o pasivamente su desempeño.
f) **Separación de responsabilidades:** Ninguna persona debe desempeñar un proceso sensible de seguridad de la información de principio a fin.

Roles y responsabilidades por nivel de acceso a la información:

El nivel de acceso del personal a la información empresarial se definirá de acuerdo con sus funciones, perfiles y roles (dueño, responsable, custodio y usuario de la información) establecidos por cada dependencia. Se propicia la gestión y la seguridad de la información mediante el establecimiento de los siguientes roles:

a) **Dueño de la información:** persona física o jurídica que tiene poder de usar y disponer de la información según la legislación, y la normativa relacionada (ICE, clientes, socios comerciales, funcionarios, trabajadores).
b) **Responsable de la información**: persona física o jurídica, que, en el ejercicio de un rol asignado por el ICE, tiene a su cargo la gestión de la información, desde su creación hasta su eliminación una vez cumplida la vigencia legal-administrativa (ciclo de vida de la información), rigiéndose por las leyes relacionadas y normativa vigente.
c) **Custodio de la información**: persona física o jurídica que, en el ejercicio de un rol asignado por el ICE, tiene la responsabilidad de custodiar la información de acuerdo con lo indicado por el responsable, rigiéndose por las leyes relacionadas y la normativa vigente.

d) **Usuario de la información:** persona física o jurídica, proceso o sistema, que, en el ejercicio de un rol asignado por el ICE, debe gestionar la información, a la cual accede de forma autorizada, de acuerdo con lo indicado por el responsable, rigiéndose por las leyes relacionadas y la normativa vigente. El nivel de acceso es designado por el responsable de la información. La información empresarial, como recurso controlado por el ICE, será valorada mediante los criterios de confidencialidad, integridad y disponibilidad con el fin de determinar los controles a establecer para su gestión y preservación.

La Dirección Ciberseguridad mediante sus procesos de Seguridad de la Información y Seguridad Informática, impulsarán una arquitectura empresarial que permita el desarrollo e implementación de controles que minimicen a niveles aceptables los riesgos de seguridad de la información y establezcan los procesos de operación correspondientes para su gestión.

La principal función del Proceso Seguridad de la Información es establecer los criterios de seguridad de la información. Para ello, utilizará metodologías para clasificar la información según los criterios establecidos en la Norma ISO/IEC 27001, Política Corporativa de Confidencialidad de la Información y las demás políticas o documentos normativos relacionados tanto a nivel corporativo como institucional o específicas para un área o proceso, además de desarrollar la metodología para la elaboración de diagnósticos de seguridad, gestión de riesgos y revisión de cumplimiento de la seguridad de la información.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

5.4 Responsabilidades de gestión

El ICE, mediante el Proceso Seguridad de la Información de la Dirección Ciberseguridad, brindará las pautas a seguir para el establecimiento, implementación, operación, seguimiento, revisión y mejora continua de los Sistemas de Gestión de Seguridad de la Información del ICE, lo cual se llevará a cabo tomando en cuenta la legislación y demás

normativa, así como estándares y/o buenas prácticas en materia de seguridad de la información y ciberseguridad.

Propósito

El ICE deberá procurar que los funcionarios y trabajadores comprendan la importancia de su participación e implementación de la seguridad de la información como parte de las obligaciones laborales.

Orientación

Los titulares subordinados deberán apoyar la implementación de este documento, mediante el aprovisionamiento de los recursos necesarios para su cumplimiento.

Para propiciar la responsabilidad en la gestión de la seguridad de la información, los titulares subordinados deberán considerar los siguientes elementos:

a) Aplicar los controles de seguridad de la información asociados a este documento.
b) Cada funcionario y trabajador tiene un papel muy importante dentro de la cultura de seguridad de la información, el Proceso Seguridad de la Información debe promover y fomentar la concientización de este tema.
c) Coordinar con el Proceso Seguridad de la Información las acciones necesarias para concientizar al personal sobre la seguridad de la información para el desarrollo de sus funciones y responsabilidades dentro de la dependencia.
d) El Proceso Seguridad de la Información establecerá metodologías y herramientas para que juntamente con las dependencias se definan las responsabilidades, para la planificación e implementación del Sistema de Gestión de Seguridad de la Información (SGSI).
e) Todas las dependencias deberán asignar recursos para la planificación del Sistema de Gestión de Seguridad de la Información, con el fin de implementar los controles de seguridad de la información.
f) Las dependencias y el personal deberán mantener constante comunicación con el fin de conocer además de gestionar sus roles y responsabilidades asociadas en seguridad de la información; así mismo, involucrar y comunicar a terceros requeridos cuando así corresponda.
g) Elaborar procedimientos documentados de acuerdo con las necesidades que se presenten durante la implementación del SGSI.
h) Las dependencias deberán llevar el control y seguimiento de la implementación del SGSI.
i) Realizar reuniones del Comité de Seguridad de la Información que se conforme como parte de la implementación del SGSI.

j) Definir los roles del SGSI de acuerdo con la matriz RACI (ver anexo No. 1), como parte de la implementación de los controles de seguridad de la información.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

5.5 Contacto con las autoridades

La institución debe establecer y mantener el contacto con las distintas autoridades que estén involucradas a nivel rector con la seguridad de información a nivel gubernamental, académico y económico.

Propósito

Establecer una adecuada comunicación entre la Institución y las distintas autoridades con la finalidad de estar en constante actualización con temas asociados a seguridad de la información, así como, contar con el soporte especializado para la gestión a los incidentes de seguridad de la información cuando corresponda.

Orientación

Identificar las autoridades pertinentes además definir cómo y cuándo se deberán notificar.

a) Las dependencias deberán identificar y documentar las autoridades correspondientes a las que se deberá acudir.

b) Definir la metodología que especifique cuándo y por medio de quiénes las autoridades (cumplimiento, leyes, organismos de reglamentación, agencia de protección de datos, así como las autoridades de supervisión) deberán contactarse de forma oportuna.

c) En caso de identificar casos de incidentes en la seguridad de la información, es necesario reportar de acuerdo con los *"Lineamientos para la Atención de Incidentes de Seguridad de la Información y Ciberseguridad".*

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
SC.CDSE.021.2019	Lineamientos para la Atención de Incidentes de Seguridad de la Información y Ciberseguridad.

5.6 Contacto con grupos de interés especial

La institución debe establecer y mantener contacto con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.

Propósito

Contar con una estrategia de comunicación y actualización con las diferentes entidades tanto nacionales como internacionales que tengan relación con la seguridad de la información, en aras de una colaboración para el mejoramiento continuo de la normativa y el accionar de la Seguridad de la Información.

Orientación

Identificar los grupos de interés en materia de seguridad de la información para contar con apoyo especializado.

El ICE mantiene puntos de enlace con encargados de ciberseguridad de otros organismos públicos y especialistas tanto internos como externos a nuestro país, que permiten estar al tanto de las tendencias, normas y métodos de ciberseguridad pertinentes (por ejemplo, el CSIRT nacional).

A nivel interno y externo de la institución, se cuenta con SLAs para asegurar la calidad de los servicios. El proceso Convenios y Alianzas de la Dirección de Comercialización de Soluciones de la GTSD coordina la elaboración de estos documentos.

El ICE debe mantener contacto con otros grupos de interés en temas de seguridad de la información como, por ejemplo; INTECO, Bomberos, Cruz Roja, Policía, Agencia Nacional de Ciberseguridad, etc., con los cuales se coordina la capacitación a nivel

mundial y certificación de personas en temas de seguridad de la información y ciberseguridad.

Algunos aspectos para tomarse en cuenta por parte de las dependencias del ICE para el cumplimiento de este requisito:

a) Las dependencias deberán identificar y documentar el contacto con grupos de interés, así como asociaciones de profesionales, a fin de mejorar el conocimiento referente a mejores prácticas, nuevas tecnologías, productos, amenazas, vulnerabilidades, agentes de amenazas, riesgos cibernéticos y mantener actualizada la información relevante sobre seguridad de la Información y seguridad informática.

b) Las dependencias deberán promover la participación en foros sobre temas de seguridad de la información y ciberseguridad, así mismo, contar con la asesoría especializada en dicha materia.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

5.7 Inteligencia sobre amenazas

La información relativa a las amenazas a la seguridad de la información y ciberseguridad debe ser recopilada y analizada para producir inteligencia.

Propósito

Proporcionar conocimiento del entorno de amenazas en la institución para que se puedan tomar las acciones de mitigación apropiadas.

Orientación

La información sobre las amenazas existentes o emergentes se recoge y se analiza. Tomando en cuenta los posibles motivos de los actores de amenazas ya que varían bastante, desde robo de dinero, minar a la competencia, robar identidades y cometer fraude, etc. Además, cada industria y organización tiene su información única que

proteger, un conjunto único de aplicaciones, tecnologías que emplean, etc. Todo ello supone un alto nivel de variabilidad en el modo en que se ejecutan los ataques, y cada día aparecen nuevos tipos.

El conocimiento del entorno de amenazas exige:

a) Comprender las amenazas que acechan a la institución y las tácticas, técnicas y procedimientos (TTP) que se utilizan para explotar sus vulnerabilidades.

b) Consultar mediante una base de conocimiento de tácticas, técnicas y procedimientos (TTP) basada en experiencias del mundo real.

c) Identificar qué información y sistemas están en riesgo, el impacto potencial al verse comprometidos y cómo dar prioridad.

d) Priorizar los objetivos de inteligencia en función de factores como qué tan cerca se apega a los valores y objetivos de la institución, qué impacto tendrá la decisión resultante y qué tan urgente es la decisión.

e) Recopilar datos sin procesar que cumplan con los requisitos previamente establecidos. Es mejor recopilar datos de una amplia gama de fuentes: internas, como registros de eventos de la red y registros de respuestas a incidentes anteriores, y externas de la web abierta, la web oscura y fuentes técnicas, a modo de construir una base de datos de conocimiento.

f) Garantizar la calidad de los datos introducidos en el sistema de inteligencia de amenazas es fundamental para el éxito general (principio de «basura entra, basura sale»).

g) Una vez que se han recopilado todos los datos sin procesar, ordenarlos y organizarlos con etiquetas de metadatos y filtrar la información redundante o los falsos positivos y negativos.

h) Para que los analistas procesen los datos de manera eficiente; la recopilación y el procesamiento de datos deben automatizarse mediante big data, aprendizaje automático e inteligencia artificial (por ej. SIEM "*Security Information and Event Management*" u otra más robusta dependiendo de la cantidad de datos administrados) para que sean de utilidad. Los datos se deben de estructurar con reglas de correlación configurables para algunos casos de uso diferentes, que facilite la identificación de sucesos sospechosos y de las tendencias actuales de ataques.

i) Para una mejor gestión de inteligencia de amenazas, establecer subcategorías como estratégica (proporciona de forma general el panorama de amenazas e informar las decisiones de alto nivel tomadas por los ejecutivos. El contenido menos técnico y se presenta a través de informes), táctica (describe las tácticas, técnicas y procedimientos (TTP) de los actores de amenazas, dirigido a personal

involucrado en seguridad de la información de la institución) y técnicas (información especializada que ayuda a los equipos de respuesta a incidentes a comprender la naturaleza, la intención y el momento de los ataques específicos).

j) Combinar correctamente las herramientas de inteligencia de amenazas y el conocimiento y criterio experto de los analistas de ciberseguridad es esencial y decisivo ante un ataque. Manteniendo la actualización tanto de las herramientas como, en la capacitación de los analistas.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

5.8 La seguridad de la información en la gestión de proyectos

El ICE debe implementar procedimientos para la gestión de proyectos, según el *Procedimiento para la Gestión de Proyectos o Épicas (GPE)* (**20.00.001.2005**), para integrar la seguridad de la información en los métodos de administración de proyectos con el fin de asegurar la identificación y abordaje de los riesgos de seguridad de la información como parte de éstos.

Propósito

Garantizar que los riesgos de seguridad de la información y ciberseguridad relacionados con los diferentes proyectos de la institución y, sus respectivos resultados se aborden de forma eficaz en la gestión de los proyectos durante su ciclo de vida.

Orientación

La seguridad de la información debe integrarse en la gestión del proyecto para garantizar que los riesgos de seguridad de la información y cibernéticos se aborden como parte de su gestión. Esto puede aplicarse a cualquier tipo de proyecto, independientemente de su complejidad, tamaño, duración, disciplina o área de aplicación (por ejemplo, un proyecto para un proceso empresarial básico, TIC, gestión de instalaciones u otros procesos de apoyo).

El integrar en la gestión de proyectos, la seguridad de la información exige:

a) Integrar la seguridad de la información en las metodologías y normativa relacionada a la gestión de proyectos para asegurar que se identifican y abordan los riesgos de seguridad de la información como parte de éstos y asegurar que la seguridad de la información sea parte de todas las fases de la metodología aplicada al proyecto.

b) Desarrollar el acta de constitución frente a la seguridad de la información, donde se describen y presentan formalmente el alcance, los límites y lineamientos generales que tendrá la gestión de la seguridad de la información durante el proyecto. Aquí el patrocinador da su aprobación y las partes se comprometen a asegurar la seguridad de la información durante el proyecto.

c) Abordar y revisar las implicaciones de seguridad de manera regular en todos los proyectos y a la vez definir y asignar las responsabilidades para la seguridad de la información a los roles especificados definidos en las metodologías de gestión de proyectos.

d) Incluir objetivos de seguridad de la información en los objetivos del proyecto.

e) Realizar un análisis de vulnerabilidades y una evaluación de riesgos de seguridad de la información en una etapa temprana del proyecto para identificar los controles necesarios relacionados a los activos de información e infraestructura involucrada.

f) Planificar los controles de Seguridad de la Información, implementar los controles de Seguridad de la Información, monitorear la eficacia de los controles de Seguridad de la Información y documentar.

g) En caso de que el proyecto se externalice parcial o totalmente, se establecen y formalizan los acuerdos de confidencialidad y acuerdo de nivel de servicio (SLA) según las normas establecidas por la institución.

h) Si durante el desarrollo o implementación del proyecto se generan nuevos requerimientos o cambios, deberán ser registrados y a la vez sometidos a un análisis de vulnerabilidades y una evaluación de riesgos de seguridad de la información.

i) Una vez finalizado la etapa de desarrollo o implementación del proyecto, se realiza una reunión con las partes involucradas e interesadas, donde se procede a conocer y analizar las lecciones aprendidas, dejando plasmado dicho acto en documento formal.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

5.9 Inventario de información y otros activos asociados

Debe elaborarse y mantenerse un inventario de activos de información y otros activos asociados, incluidos los propietarios.

Propósito

Identificar la información de la institución y otros activos asociados con el fin de preservar la seguridad de la información y asignar la responsabilidad adecuada.

Orientación

El Proceso Seguridad de la Información, junto con los funcionarios y trabajadores, según sus responsabilidades, deben identificar los activos de información e infraestructura tecnológica y determinar su importancia en términos de seguridad de la información. La documentación debe mantenerse en inventarios dedicados o existentes, según corresponda. Este inventario debe ser preciso, estar actualizado, ser coherente y estar alineado con las normas respectivas.

Para tal efecto se debe:

a) Gestionar la seguridad de la información en la institución, mediante la definición, implementación, seguimiento y mejoramiento de elementos (herramientas, controles, procedimientos, guías, instructivos y líneas base.) que permitan proteger la información frente a la posible materialización de riesgos que afecten su confidencialidad, integridad y disponibilidad (CIA) sin importar el orden de esta o priorizando según el negocio.

b) Identificar los activos de información e infraestructura tecnológica en la que al menos se incluya el nombre único del proceso, la descripción del proceso, las actividades asociadas (creadas, almacenadas, transmitidas, eliminadas), la criticidad del proceso (si es crítico, de apoyo, etc.), el responsable del proceso

(unidad de organizacional), los procesos que proveen entradas y salidas de ese proceso, la infraestructura tecnológica que apoya el proceso.

c) Establecer la clasificación de la información según corresponda para preservar la confidencialidad, integridad, disponibilidad, control de acceso, no repudio y/u otras propiedades que la institución considere importantes, por ejemplo, cuánto tiempo puede almacenarse los activos de información.

d) Una vez identificados los activos de información e infraestructura tecnológica (documentación, servicios de comunicación, hardware, software, instalaciones, personas), se debe definir el responsable de los activos de información, definir el custodio de los activos de información, definir los usuarios de los activos de información y consolidar los activos de información en un “inventario de activos de información e infraestructura tecnológica”.

e) Las políticas, lineamientos y cualquier normativa aprobada deben ser difundidos, incorporados y acogidos al interior de cada dependencia, las cuales, junto con las normas internacionales asociadas, son la base para que se implemente la gestión de la seguridad de la información de la institución.

f) La institución por medio del Proceso Seguridad de la Información propondrá las mejores prácticas para la gestión de la seguridad de la información, como mecanismo para proteger los activos de información e infraestructura tecnológica.

g) Por ser la información el activo más importante de la institución, es necesario protegerla frente a los posibles riesgos derivados del uso de las nuevas tecnologías, para garantizar la seguridad de la información, en aspectos tales como confiabilidad, integridad y disponibilidad de ésta.

h) Para efectos de la gestión documental y archivística, en cumplimiento de la legislación y la normativa interna, se debe identificar la documentación que se produce en el desarrollo de las actividades de la institución, determinar su valor como activos de información, respetar los tiempos de retención hasta su disposición final (tablas de retención), según lo dicte la dependencia competente en esta materia.

i) Para los tipos de activos de información personas, cuando corresponda también se debe tomar en cuenta el conocimiento, en especial del personal clave, en razón que estos temas requieren de análisis específicos y especializados relacionados con el manejo y desarrollo del talento humano y la gestión del conocimiento en la institución.

j) Por medio de los sistemas de información se recogen datos, que de una u otra forma, transformados en información, tienen injerencia en la resolución de los asuntos necesarios para la continuidad del negocio en este escenario las bases

de datos, relacionadas entre sí y estructuradas permiten el rápido acceso, manipulación y extracción de los datos, por lo que requieren de una identificación, protección, control y seguimiento en términos de acceso, confidencialidad, integridad y disponibilidad de los datos, por lo tanto éstas pueden registrarse como activos de información tipo datos o documentación.

k) El conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas, se constituyen en información y base de conocimientos dadas al computador y que son requeridas para el trabajo de estos sistemas, por lo tanto, éstas pueden registrarse como activos de información tipo software.

l) El componente físico de los sistemas de información y comunicación es el medio utilizado para realizar la captura, procesamiento, almacenamiento, difusión y divulgación de la información, en este sentido, se refiere a todos los elementos físicos que permiten el correcto funcionamiento de un medio informático. Incluye discos duros o extraíbles, impresoras, computadoras, dispositivos móviles, entre otros. Para facilidad de manejo de este tipo de activos, los mismos pueden ser agrupados según sus características y ser registrados como activos de información tipo hardware.

m) Aquellos medios de soporte a los activos de información, que facilitan la administración o flujo de la información generada por el proceso, como la red, los servidores, los switches, la intranet, el internet, el VPN, el correo electrónico, entre otros, pueden registrarse como activos de información tipo servicios de comunicación.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

5.10 Uso aceptable de la información y otros activos asociados

Deben identificarse, documentarse y aplicarse normas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados.

Propósito

Procurar que la información y otros activos de la institución sean protegidos y se utilicen adecuadamente.

Orientación

El personal y demás usuarios que tengan acceso a la información y activos de la institución deben conocer y acatar las medidas de seguridad de la información que se hayan emitido para proteger y manipular la información y sus activos.

La institución debe establecer los requerimientos de seguridad para la protección de los activos y la información almacenada y accedida por medio de dispositivos con el fin de preservar la confidencialidad, integridad y disponibilidad de la información almacenada y accedida por estos dispositivos.

Para tal efecto se debe:

a) Elaborar procedimientos para el uso de la información, que incluyan los perfiles de acceso, restricciones de los usuarios y el proceso para la eliminación.

b) La información, los activos asociados y otros recursos informáticos puestos a disposición del usuario(a) serán para uso exclusivo de sus funciones laborales y son propiedad de la institución.

c) Mantener un registro de los usuarios que tienen acceso a la información.

d) Garantizar que los funcionarios, trabajadores o terceros conozcan la responsabilidad sobre la información empresarial y los activos, así como las medidas de seguridad, confidencialidad y respaldo según corresponda.

e) Los equipos o medios que sean utilizados para almacenar, procesar o comunicar la información deben mantener las medidas de protección físicas y lógicas que se hayan identificado como necesarias para mantener un monitoreo en apego a la normativa establecida y un correcto estado de funcionamiento. Cuando sean utilizados medios de almacenamiento de información de uso común, los usuarios deben eliminar la información de estos dispositivos una vez finalizado su uso, y así evitar que otros usuarios tengan conocimiento o acceso a ésta.

f) El manejo de información empresarial mediante dispositivos móviles debe realizarse conforme al Reglamento para la Utilización de la Información del ICE mediante Dispositivos Móviles.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
87.00.001.2022	Reglamento para la Utilización de la Información del ICE mediante Dispositivo Móviles.

5.11 Devolución de activos

El personal y otras partes interesadas, según corresponda, deben devolver todos los activos de información que estén en su poder al cambiar de funciones o terminar su relación laboral, contrato o acuerdo, según corresponda.

Propósito

Proteger los activos de la institución como parte del proceso de cambio, daño, obsolescencia o bien por terminación o modificación de las funciones del funcionario o trabajador, sea por cambio de labores en las que no lo amerita debido a su nuevo perfil o retiro de la institución, así como por terminación de la relación contractual.

Orientación

El proceso de cambio o terminación debe formalizarse para incluir la devolución de todos los activos físicos y electrónicos emitidos que sean propiedad de la institución y que se le hayan confiado.

La institución debe identificar y documentar claramente toda la información y otros activos asociados que deben ser devueltos, incluyendo la cláusula de devolución de activos físicos y/o electrónicos y debe incluir, entre otros:

a) Dispositivos de punto final del usuario;
b) Dispositivos de almacenamiento portátiles;
c) Equipo especializado;
d) Hardware de autenticación (por ejemplo, llaves mecánicas, tokens físicos y tarjetas inteligentes) para sistemas de información, sitios y archivos físicos;
e) Copias físicas de la información.

La institución debe establecer procedimientos de transferencia y borrado de información de forma segura en el caso que sea pertinente (Uso de equipos propios, transferencia y devolución de equipos, etc.)

El personal y otras partes interesadas, según corresponda, deben devolver todos los activos en su poder al cambiar o terminar su relación laboral, contrato o acuerdo o bien si sus actividades cambian y estos activos no son requeridos, tal como lo estipula la normativa de uso de activos institucionales o bien las obligaciones contractuales.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
61.00.004.2014	Reglamento para el Registro, Uso, Custodia y Control de Activos Muebles.
87.00.001.2022	Reglamento del Uso de Información del ICE mediante Dispositivos Móviles.

5.12 Clasificación de la información

La información debe clasificarse según las necesidades de seguridad de la información de la institución, basándose en la confidencialidad, la integridad, la disponibilidad y en los requisitos que establezcan las partes interesadas en el ejercicio de sus competencias y los establecidos internamente.

Propósito

Asegurar la identificación y la comprensión de las necesidades de protección de la información de acuerdo con su importancia para la institución.

Orientación

La institución debe establecer normativa de temas específicos sobre la clasificación de la información y comunicarla al personal. Tratándose de proveedores y socios comerciales deberá incluirse en el pliego de condiciones o el contrato la obligación de rendir una declaración jurada en la que se comprometen a acatar la normativa interna en materia de

seguridad de la información, incluida la que regule esta temática, a mantenerse actualizados de todas las modificaciones o reformas de las disposiciones o documentos normativos en la materia, incluyendo la citada política, cuando se publiquen en el Diario Oficial La Gaceta, en caso contrario (cuando no se publique en la Gaceta), el administrador del contrato, debe comunicárselas. La institución debe tener en cuenta los requisitos de confidencialidad, integridad y disponibilidad en el esquema de clasificación.

La información del ICE debe clasificarse según el Modelo de Objetos y Datos a Nivel Conceptual de la Institución. La clasificación asegura conocer la criticidad e importancia de la información. Se debe considerar tanto, un análisis de riesgo que permita identificar el impacto asociado a la pérdida de información, así como un plan de recuperación ante desastres que garantice la continuidad operativa de los servicios.

La información debería clasificarse según:

a) Su valor para la institución (Modelo de Objetos y Datos).
b) Los requisitos legales (Datos personales, Información Sensible, otros).
c) Nivel de Protección necesario: Su criticidad y sensibilidad en cuanto a su divulgación o modificación no autorizada o accidental.

El responsable de la clasificación de la información es el propietario del activo de información, según el apartado 8.1.2 Propiedad de los Activos, norma ISO 27001.

Algunos aspectos por tomar en cuenta;

a) El esquema de clasificación debe ser uniforme para toda la institución.
b) El esquema de clasificación debe alinearse con la política de control de acceso.
c) El nivel de protección debe ser evaluado según los criterios de confidencialidad, integridad y disponibilidad.
d) La clasificación de la información debe revisarse periódicamente y mantenerse actualizada.

Otras consideraciones

Podría agruparse por tipos de activos o información con requisitos de protección similares de forma que no se tenga que realizar una especificación de procedimientos de seguridad de la información caso a caso sino para un grupo de activos de información similares.

La norma ISO 270001 proporciona un ejemplo para **la clasificación de la criticidad** de la información en relación con la confidencialidad:

- **Nivel 0** la divulgación no causa ningún daño.
- **Nivel 1** la divulgación causa menor incomodidad o inconveniencia operativa menor.

- **Nivel 2** la divulgación tiene un impacto significativo a corto plazo en las operaciones o los objetivos tácticos.
- **Nivel 3** la divulgación tiene un grave impacto en los objetivos estratégicos a largo plazo o pone en riesgo la supervivencia de la institución.

Otra consideración para tomar en cuenta es con respecto a la gestión de la información declarada confidencial la cual estará regulada por el documento normativo que al efecto se emita.

Documentos Relacionados

Código	Ley, Política, Norma
Ley 8968	Ley de Protección de las Persona frente al tratamiento de sus Datos.
Ley 7202	Ley del Sistema Nacional de Archivos.
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
ISO 27001:2022	Apartado 8.1.2 Propiedad de los Activos.
19.00.001.2017	Lineamientos para el Funcionamiento del Modelo de Arquitectura de Información Empresarial para el Grupo ICE.
76.00.001.2016	Procedimiento para la Actualización del Modelo de Objetos y Datos a Nivel Conceptual.
48.00.001.2017	Procedimiento para la Actualización del Tesauro Especializado en Electricidad y Telecomunicaciones.
Decreto Ejecutivo 40554	Reglamento a la Ley del Sistema Nacional de Archivos.
48.00.007.2010	Manual para el Funcionamiento del Modelo Archivístico Institucional.

5.13 Etiquetado de la información

Debe desarrollarse y aplicarse un conjunto adecuado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información adoptado por la institución.

Propósito

Para facilitar la comunicación de la clasificación de la información y apoyar la automatización del procesamiento y la gestión de la información.

Orientación

Los procedimientos de etiquetado de la información deben abarcar la información y otros activos asociados en todos los formatos. Las etiquetas deben ser fácilmente reconocibles. Los procedimientos deben orientar sobre dónde y cómo se colocan las etiquetas teniendo en cuenta cómo se accede a la información o se manejan los activos en función de los tipos de soportes de almacenamiento.

La información debería ser etiquetada de acuerdo con el esquema de clasificación que se haya definido según el apartado anterior.

El proceso de etiquetado puede tener excepciones (Activos que no necesiten etiquetado, por ejemplo, se puede evitar tener que poner la etiqueta: “Información no confidencial”), algo que tiene que estar especificado en un procedimiento de etiquetado.

Los activos de los sistemas que contienen información clasificada como sensible o crítica deberían llevar una etiqueta adecuada de clasificación.

El etiquetado de la información clasificada es un requisito clave para acuerdos que impliquen compartir información.

Los requisitos son:

- El etiquetado afecta a la información y sus activos relacionados en formato físico y electrónico.
- Debe realizarse según el esquema de clasificación definido en el punto anterior.
- Las etiquetas deben reconocerse fácilmente.

El etiquetado de la información puede realizarse de forma física o por medio de metadatos.

Se debe tener en cuenta que, el etiquetado de los activos es una herramienta útil para el reclamo en caso de uso indebido de información por usuarios no autorizados.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
ISO 27001:2022	Apartado 8.1.2 Propiedad de los Activos.
19.00.001.2017	Lineamientos para el Funcionamiento del Modelo de Arquitectura de Información Empresarial para el Grupo ICE.
76.00.001.2016	Procedimiento para la Actualización del Modelo de Objetos y Datos a Nivel Conceptual.
48.00.001.2017	Procedimiento para la Actualización del Tesauro Especializado en Electricidad y Telecomunicaciones.
Ley 7202	Ley del Sistema Nacional de Archivos.
Decreto Ejecutivo 40554	Reglamento a la Ley del Sistema Nacional de Archivos.
48.00.007.2010	Manual para el Funcionamiento del Modelo Archivístico Institucional.

5.14 Transferencia de información

Deben existir normas, procedimientos o acuerdos de transferencia de información para todo tipo de transferencia de información física y digital dentro de la institución y entre ésta y otras partes.

Propósito

Mantener la seguridad de la información durante el intercambio y transferencia dentro de la institución y con cualquier parte externa interesada.

Orientación

La institución debe establecer y comunicar al personal una normativa específica sobre la transferencia de información. Tratándose de proveedores y socios comerciales deberá

incluirse en el pliego de condiciones o el contrato la obligación de rendir una declaración jurada en la que se comprometen a acatar la normativa interna en materia de seguridad de la información, incluida la que regule esta temática, a mantenerse actualizados de todas las modificaciones o reformas de las disposiciones o documentos normativos en la materia, incluida esta política, cuando se publiquen en el Diario Oficial La Gaceta, en caso contrario (cuando no se publique en la Gaceta), el administrador del contrato, debe comunicárselas.

Las normas, procedimientos y acuerdos para proteger la información en tránsito deben reflejar la clasificación de la información en cuestión. Cuando la información se transfiera entre la institución y terceros, deben establecerse y mantenerse acuerdos de transferencia (incluyendo la autentificación del receptor) para proteger la información en todas sus formas en tránsito.

La transferencia de información puede producirse a través de la transferencia electrónica, la transferencia en medios de almacenamiento físico y la transferencia verbal.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
ISO 27001:2022	Apartado 8.1.2 Propiedad de los Activos.
19.00.001.2017	Lineamientos para el Funcionamiento del Modelo de Arquitectura de Información Empresarial para el Grupo ICE.
76.00.001.2016	Procedimiento para la Actualización del Modelo de Objetos y Datos a Nivel Conceptual.
48.00.001.2017	Procedimiento para la Actualización del Tesauro Especializado en Electricidad y Telecomunicaciones.
Ley 7202	Ley del Sistema Nacional de Archivos.

Código	Ley, Política, Norma
Decreto Ejecutivo 40554	Reglamento a la Ley del Sistema Nacional de Archivos.
48.00.007.2010	Manual para el Funcionamiento del Modelo Archivístico Institucional.

5.15 Control de acceso

Las reglas para controlar el acceso físico y lógico a la información y a otros activos asociados deben establecerse e implementarse basándose en los requisitos de seguridad de la empresa y de la información.

Propósito

Garantizar que el acceso a la información y a otros activos asociados sea definida y autorizada de acuerdo con los requisitos establecidos por la institución.

Orientación

Las reglas para controlar el acceso físico y lógico a la información y a otros activos asociados deben establecerse e implementarse basándose en los requisitos de seguridad de la empresa y de la información.

Con el fin de regular a nivel institucional el control de acceso a las distintas instalaciones se ha elaborado varios documentos que marcan las pautas a seguir y las recomendaciones según sea el caso.

- **Seguridad física:** Relativo a la protección y control de bienes institucionales de las instalaciones, personas y operaciones habituales del ICE, contra acciones delictivas o cualquier otra amenaza o riesgo.
- **Seguridad lógica:** Se refiere a la aplicación de medidas de protección para el resguardo de la infraestructura tecnológica y sus datos, ante incidentes de seguridad y accesos no autorizados.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.

Código	Ley, Política, Norma
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
10.00.0001.2009	Reglamento General de Acceso y Tránsito a Instalaciones del Instituto Costarricense de Electricidad.
10.00.002.2009	Reglamento para el Uso de Carné Corporativo de las Empresas del Grupo ICE.
36.00.001.2009	Reglamento para la Utilización de Recursos Informáticos del Usuario Final: Hardware, Software y Servicio de Comunicaciones. En el apartado 6.7.

5.16 Gestión de la identidad

Debe gestionarse el ciclo de vida completo de las identidades.

Propósito

Permitir la identificación única de las personas y los sistemas que acceden a la información del ICE y otros activos asociados, así como permitir la asignación adecuada de los derechos de acceso.

Orientación

Los procesos utilizados en el contexto de la gestión de la identidad deben garantizar:

a) En el caso de las identidades asignadas a personas, una identidad específica sólo está vinculada a una única persona para poder responsabilizarla de las acciones realizadas con esta identidad específica.
b) Las identidades asignadas a entidades no humanas están sujetas a una aprobación debidamente segregada y a una supervisión continua independiente.
c) Las identidades se desactivan o eliminan oportunamente si ya no son necesarias.
d) En un dominio específico, una sola identidad se asigna a una sola entidad.
e) Se mantienen registros de todos los eventos significativos relativos al uso y la gestión de las identidades de los usuarios y de la información de autenticación.
f) Las cuentas de usuario serán restringidas o limitadas específicamente a lo que le compete a su titular para llevar a cabo sus actividades, basado en el principio de mínimo privilegio.
g) Las cuentas de administración del fabricante, creadas por defecto en los equipos de servicios de información tales como administrador, entre otros, serán utilizadas

por los usuarios solo en casos debidamente justificados; las cuentas genéricas, default o root por defecto no deberá de existir en los sistemas.

h) Cada dependencia, según corresponda, será responsable de notificar de inmediato el cese o cambio de funciones del personal de la institución, finalización de contratos con proveedores o socios comerciales a la dependencia encargada de administrar las cuentas de usuario.

i) Las cuentas de usuario serán creadas, modificadas, inhabilitadas y eliminadas por las dependencias encargadas de dichas cuentas, de acuerdo con los procedimientos establecidos, según corresponda a cada área.

j) Se debe llevar a cabo una revisión periódica de los privilegios de usuarios en los sistemas, que permita verificar su validez. Esta revisión se debe realizar por parte de las dependencias encargadas de administrar las identidades y privilegios de seguridad de la información, en coordinación con los responsables de la información.

k) La dependencia que haga uso de un servicio de información gestionará mediante procedimientos establecidos y en coordinación con los responsables de la información los usuarios y privilegios requeridos.

l) Los usuarios que administren activos de soporte deben de contar con una cuenta con privilegios especiales no más allá de los que necesita para ejercer su gestión.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
87.00.002.2021	Procedimiento para la Administración de los Accesos a los Sistemas Transaccionales del ICE.

5.17 Información de autentificación

La asignación y gestión de la información de autenticación debe ser controlada por un proceso de gestión, que incluya el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.

Propósito

Garantizar la correcta autentificación de las entidades y evitar fallos en los procesos de autentificación.

Orientación

El proceso de asignación y gestión debe garantizar que:

a) Se establecen procedimientos para verificar la identidad de un usuario antes de proporcionar información de autenticación nueva, de sustitución o temporal.

b) La información de autentificación, incluida la información de autentificación temporal, se transmite a los usuarios de forma segura y se evita el uso de mensajes de correo electrónico no protegidos para este fin. Los usuarios acusan recibo de la información de autenticación.

c) La información de autentificación por defecto, tal y como está predefinida o proporcionada por los proveedores, se cambia inmediatamente después de la instalación de los sistemas o del software.

d) Se mantengan registros de los eventos significativos relativos a la asignación y gestión de la información de autenticación y que se garantice su confidencialidad, y que el método de mantenimiento de registros esté aprobado.

Cualquier persona o entidad que tenga acceso a la información de autenticación o la utilice, debe asegurarse de:

a) Mantener confidencial toda la información de autenticación e identificación, salvo casos especiales, cuando ésta sea vinculada a múltiples usuarios o entidades no personales, en este caso, se comparte únicamente con las personas autorizadas.

b) Cambiar inmediatamente la información de autenticación afectada o comprometida tras la notificación o cualquier otro indicio de compromiso.

c) Seleccionar contraseñas robustas cuando se utilizan como información de autenticación, de acuerdo con las recomendaciones de las mejores prácticas.

d) No utilizar las mismas contraseñas en distintos servicios y sistemas.

Cuando las contraseñas se utilizan como información de autenticación, el sistema de gestión de contraseñas debería:

a) Permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación para hacer frente a los errores de introducción.

b) Aplicar contraseñas seguras según lo establecido por la Institución.

c) Obligar a los usuarios a cambiar sus contraseñas en el primer acceso.

d) Aplicar los cambios de contraseña que sean necesarios, por ejemplo, después de un incidente de seguridad, o en caso de cese o cambio de empleo cuando un usuario tenga contraseñas conocidas para identidades que permanezcan activas.
e) Evitar la reutilización de contraseñas anteriores.
f) Evitar el uso de contraseñas de uso común y de nombres de usuario comprometidos.
g) No mostrar las contraseñas en la pantalla cuando se introducen.
h) Almacenar y transmitir las contraseñas de forma protegida.
i) El cifrado y el hash de las contraseñas deben realizarse de acuerdo con las técnicas criptográficas aprobadas para las contraseñas.
j) Las dependencias encargadas de administrar las cuentas de usuarios deben contar con procedimientos aprobados para la gestión y el control de contraseñas.
k) El sistema o sistemas de administración de contraseñas, deberá proporcionar los mecanismos necesarios para verificar la integridad, confidencialidad y disponibilidad de las contraseñas.
l) Los usuarios serán responsables de las actividades realizadas a través de su cuenta de usuario.
m) El acceso a los servicios de información por parte de cada usuario de acuerdo con las posibilidades técnicas del ICE se realizará por medio de un único identificador de usuario.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
87.00.002.2021	Procedimiento para la Administración de los Accesos a los Sistemas Transaccionales del ICE.

5.18 Credenciales de acceso

Las credenciales de acceso a la información y a otros activos asociados deben ser aprovisionados, revisados, modificados y eliminados de acuerdo con la política específica del ICE sobre el tema y las reglas para el control de acceso.

Propósito

Garantizar que el acceso a la información y a otros activos asociados se defina y autorice de acuerdo con los requisitos de la Institución.

Orientación

Provisión y revocación de derechos de acceso

El proceso de aprovisionamiento para asignar o revocar los derechos de acceso físico y lógico concedidos hacia una entidad debe incluir:

a) Obtener la autorización del propietario de la información y de otros activos asociados para el uso de éstas. También puede ser conveniente la aprobación por separado de los derechos de acceso por parte del custodio de la información o bien el responsable de administración.

b) Considerar los requisitos de la normativa institucional vigente en materia de control de acceso.

c) Considerar la segregación de funciones, incluyendo la segregación de los roles de aprobación y aplicación de los derechos de acceso y la separación de los roles conflictivos.

d) Garantizar que los derechos de acceso se eliminen cuando alguien no necesite acceder a la información y a otros activos asociados, en particular, garantizar que los derechos de acceso de los usuarios que han dejado la Institución se eliminen en el momento oportuno.

e) Considerar la posibilidad de conceder derechos de acceso temporales por un período de tiempo limitado y revocarlos en la fecha de expiración.

f) Verificar que el nivel de acceso concedido se ajusta a los documentos normativos de control de acceso y es coherente con otros requisitos de seguridad de la información, como la separación de funciones.

g) Garantizar que los derechos de acceso se activen sólo después de que los procedimientos de autorización se hayan completado con éxito.

h) Mantener un registro central de los derechos de acceso concedidos a un usuario para acceder a la información y a otros activos asociados.

i) Modificar los derechos de acceso de los usuarios que han cambiado de función o concluido su relación laboral con el ICE o con el proveedor o socio comercial.

j) Eliminar o ajustar los derechos de acceso físicos y lógicos, lo que puede hacerse mediante la eliminación, revocación o sustitución de claves, información de autenticación, suscripciones.
k) Mantener un registro de los cambios en los derechos de acceso lógico y físico de los usuarios.

Revisión de los derechos de acceso:

Las revisiones periódicas de los derechos de acceso físicos y lógicos deben tener en cuenta lo siguiente:

a) Los derechos de acceso de los usuarios, después de cualquier cambio de funciones dentro de la Institución o de la terminación de la relación laboral o contractual.
b) Autorizaciones de derechos de acceso privilegiados.

Consideración antes del cambio o de la terminación del empleo:

Los derechos de acceso de un usuario a la información y a otros activos asociados deben ser revisados, ajustados o eliminados antes de cualquier cambio o cese de empleo, basándose en la evaluación de factores de riesgo como:

a) Si la terminación o el cambio es iniciado por el usuario o por la jefatura formal correspondiente y el motivo de la terminación.
b) Las responsabilidades actuales del usuario.
c) El valor de los activos actualmente accesibles.

Se contará con controles para la manipulación de los activos de información, con base en su nivel de clasificación, de acuerdo con las potestades de los roles establecidos y considerando los siguientes aspectos:

a) Acceso de sólo lectura.
b) Acceso a escritura (incluyendo lectura).
c) Acceso de modificación (incluyendo lectura y escritura).

El administrador de sistemas llevará a cabo la creación, la actualización y la eliminación de los accesos y privilegios de usuario a los sistemas y las aplicaciones, con previa solicitud de los responsables de las clases de activos de información.

El acceso a los servicios de información se realizará mediante un procedimiento formal a través de un inicio seguro de sesión.

Se deberá limitar el tiempo máximo y mínimo para el inicio de sesión. Si se excede el tiempo establecido, el sistema finalizará automáticamente el proceso de inicio de sesión.

Los administradores de archivos de gestión y archivo central de información con soporte documental mantendrán un inventario de los accesos y privilegios de usuario a la información custodiada con la autorización respectiva de los responsables de las clases de activos de información.

Se deben de contemplar los siguientes aspectos:

a) Requisitos de seguridad de las aplicaciones.
b) Identificación de toda la información relativa a las aplicaciones.
c) Coherencia entre normativas de control de accesos y las normativas de clasificación de la información.
d) Obligaciones legales que pueden derivarse.
e) Perfiles estándar de usuarios para tareas habituales.
f) Gestión de derechos de accesos en un entorno de red en el que se reconozca todo el tipo de conexiones disponibles.
g) Segregación de roles de control de acceso.
h) Anulación de derechos de acceso.

Salvo excepciones, la gestión de los accesos a las plataformas y, aplicaciones se llevará a cabo dentro de alguno de los repositorios centralizados. En estos repositorios los usuarios tendrán asociado un identificador único en el que se especificará a qué aplicaciones se tiene acceso y con qué privilegios. Sólo los administradores de la plataforma o aplicación tendrán acceso a estos repositorios, y los cambios en los perfiles deberán ser solicitados por los responsables de la dependencia siguiendo el Procedimiento de Gestión de Cambios.

Revisión de derechos de acceso

a) Los derechos de acceso serán revisados en las auditorías de conformidad técnica por parte del responsable de la gestión de los accesos y el titular subordinado involucrado.
b) Las dependencias encargadas de la operación y mantenimiento de las infraestructuras, comunicaciones y accesos deberán tener en cuenta las siguientes pautas para la revisión de los derechos de acceso de los usuarios:
    - Revisar periódicamente, y siempre después de cualquier cambio de funciones o por finalización de la relación laboral y contractual.
    - Los derechos de usuario serán revisados y reasignados cuando haya un cambio de puesto de trabajo.
    - Las autorizaciones para privilegios especiales deben ser revisadas como mínimo una vez al año.

- Las asignaciones de privilegios deben ser comprobadas a intervalos regulares para asegurar que nadie ha obtenido privilegios no autorizados (al menos una vez al semestre).
- Los cambios de privilegios deben ser registrados, debe quedar evidencia de los cambios realizados.
- La revisión de derechos de acceso es realizada por el responsable del activo de información, mediante una auditoría de conformidad técnica y con notificación de los resultados al responsable de seguridad de la información y al titular subordinado.

En caso de que se encuentre alguna incidencia, además de registrarlo en el informe de auditoría de conformidad técnica, debe comunicar esta situación los responsables del activo, y si procede, debe abrir una acción de no conformidad.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
87.00.002.2021	Procedimiento para la Administración de los Accesos a los Sistemas Transaccionales del ICE.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.

5.19 Seguridad de la información en las relaciones con los proveedores

Deben definirse y aplicarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados al uso de los productos o servicios del proveedor o socio comercial.

Propósito

Mantener un nivel de seguridad de la información en las relaciones con los proveedores o socios comerciales, según lo especificado en el pliego de condiciones o en el contrato correspondiente.

Orientación

Implementar medidas de seguridad de la información en especial al tratamiento de la información confidencial o privada en los procesos de contratación administrativa, relaciones con proveedores, asociaciones empresariales, entre otros, en referencia a las leyes y normativa de contratación pública.

Para ello se debe:

a) Poner especial atención en evaluar la criticidad de todos los servicios susceptibles de ser contratados de manera que puedan identificarse aquellos que sean relevantes desde el punto de vista de la seguridad de la información, ya sea por su naturaleza, la sensibilidad de los datos que deban tratarse o la dependencia sobre la continuidad de negocio.

b) Cuidar los procesos de selección de los proveedores, socios comerciales, requerimientos contractuales como la terminación contractual, el monitoreo de los niveles de servicio, la devolución de información y las medidas de seguridad implantadas por dicho proveedor, que deberán ser, al menos, equivalentes a las que se establecen en el presente documento.

c) El pliego de condiciones o los contratos que por su naturaleza lo requieran, deberían, con fundamento en las condiciones de la contratación o de la elección del socio, prever cláusulas de : devolución o destrucción de la información o activos al final del contrato, procedimientos de salida y de traslado de información en caso de ruptura de la relación contractual, prohibición de acceso sin autorización explícita y mantenimiento de una lista de individuos con accesos, cláusulas de confidencialidad, obligatoriedad de firmar acuerdos de no revelación por parte de los empleados/agentes del proveedor, entre otros.

d) Definir la información del ICE, los servicios TIC y la infraestructura física a la que los proveedores pueden acceder, supervisar, controlar o utilizar.

e) Definir los tipos de componentes de la infraestructura de las TIC y los servicios prestados por los proveedores que pueden afectar la confidencialidad, integridad y disponibilidad de la información de la institución.

f) Evaluar y gestionar los riesgos de seguridad de la información relacionados con:
   - El uso de la información del ICE por parte del proveedor o socio comercial.
   - Riesgos originados por el personal del proveedor o del socio comercial.

- Vulnerabilidades de los productos o los servicios prestados por los proveedores.

g) Manejo de incidentes y contingencias asociados a los productos y servicios de los proveedores o socios comerciales, incluyendo las responsabilidades tanto del ICE como de los proveedores o socios comerciales.

h) Coordinar con el Proceso Seguridad de la Información la concientización y formación para el personal del ICE que interactúa con el personal de los proveedores o socios comerciales, referente a la aplicación de buenas prácticas seguridad de la información, legislación y documentos relacionados.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
Ley 9986	Ley General de Contratación Pública.
Decreto Ejecutivo 43808	Reglamento a la Ley General de Contratación Pública.
16.00.002.2022	Reglamento Interno de Contratación Pública ICE.
36.00.003.2018	Reglamento Interno de Contratación Administrativa ICE.
IT-PA-004	Instructivo de Trabajo para los Archivos de Contratación Administrativa.

5.20 Abordar la seguridad de la información en los contratos con los proveedores y socios comerciales

Deben establecerse y acordarse con cada proveedor o socio comercial, en el pliego de condiciones o en los contratos, los requisitos pertinentes en materia de seguridad de la información en función del tipo de relación.

Estos requisitos deben establecerse también a los oferentes, cuando por la naturaleza de la contratación se requiera que tengan acceso a determinada información empresarial, previo a la adjudicación o firma de contrato.

Propósito

Implementar controles de seguridad de la información en las relaciones con los oferentes cuando así corresponda, proveedores o socios comerciales.

Orientación

Los acuerdos con los oferentes, cuando así corresponda, o los contratos con los proveedores o socios comerciales deberán documentarse con el fin de garantizar que exista un claro entendimiento sobre las obligaciones de ambas partes de cumplir con los controles de seguridad de la información.

Acuerdos como los que se detallan en los siguientes puntos:

a) En los contratos o acuerdos con los oferentes, cuando así proceda, proveedores y socios comerciales se debe incluir una cláusula de confidencialidad de la información.

b) En las relaciones contractuales con terceros, se debe firmar un contrato de confidencialidad, dónde se delimiten las obligaciones de ambas partes receptor de información y revelador de información.

c) Los proveedores y socios comerciales solo podrán tener acceso a los activos de información necesarios para el desarrollo de sus obligaciones contractuales.

d) El acceso de proveedores y socios comerciales a los sistemas de información estará definido por usuario y contraseña el cual tendrá el nivel de acceso requerido para el desarrollo de sus obligaciones contractuales.

e) Los proveedores y socios comerciales, así como los empleados de éstos, al dejar de prestar sus servicios a la Institución, o bien terminar la relación laboral o contractual según corresponda, deben entregar toda información del producto del trabajo realizado y hacer entrega de los equipos y recursos tecnológicos en perfecto estado, de acuerdo con las condiciones establecidas en el contrato o convenio. Terminada la relación contractual, tanto el proveedor, el socio comercial, como sus empleados, mantienen el compromiso de no utilizar, comercializar o divulgar, directamente o a través de terceros, la información generada o conocida durante la relación con la Institución.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC

Deben definirse y aplicarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados a la cadena de suministro de productos y servicios de TIC.

Propósito

Mantener un nivel acordado de seguridad de la información en las relaciones con los proveedores o socios comerciales, según lo especificado en el pliego de condiciones o en el contrato correspondiente.

Orientación

a) Los contratos con los proveedores o socios comerciales deben incluir los requisitos para abordar los riesgos de seguridad de la información y las comunicaciones, además en la cadena de suministro del producto a considerar.

b) Para los servicios de tecnologías de la información y comunicaciones, los proveedores o socios comerciales y los empleados a su cargo deberán aplicar las mejores prácticas de seguridad de la información en toda la cadena de suministro de productos y servicios que son entregados al ICE.

c) Implementar procesos de seguimiento y monitoreo con el fin de validar la entrega de información, productos y servicios que se adhieran a los requisitos de seguridad de la información.

d) Identificar componentes de productos y servicios que sean críticos para mantenimiento y funcionabilidad, por lo que es necesario establecer un mayor control.

e) Implementar procesos para la gestión de tecnologías de la información y comunicaciones, el ciclo de vida de los componentes y los riesgos asociados.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

5.22 Seguimiento, revisión y gestión de cambios de los servicios de los proveedores

La institución debe supervisar, revisar, evaluar y gestionar regularmente los cambios en las prácticas de seguridad de la información de los proveedores o socios comerciales, según lo especificado en el pliego de condiciones o en el contrato correspondiente.

Propósito

Implementar la seguridad de la información en la prestación de servicios conforme a los contratos con los proveedores o socios comerciales.

Orientación

El seguimiento, la revisión y la gestión de los cambios de los servicios de los proveedores o socios comerciales, deben garantizar que se cumplan los términos y condiciones de seguridad de la información de los contratos, que los incidentes y problemas de seguridad de la información se gestionen de forma adecuada y que los cambios que surjan en los servicios de los proveedores, socios comerciales o en la situación de la empresa no afecten a la prestación del servicio. Para tal efecto se debe:

a) Gestionar los cambios al suministro de los servicios por parte de los proveedores o socios comerciales, incluyendo el mantenimiento, mejora de políticas, procedimientos, controles a considerar además de la criticidad de la información del servicio, sistemas y los procesos involucrados así mismo, la reevaluación de los riesgos considerando lo siguiente:
    - *Cambio en los contratos con los proveedores o socios comerciales.*
    - *Cambios para poner en práctica las* mejoras en los servicios ofrecidos, desarrollo de nuevas aplicaciones y sistemas, modificación en las políticas o procedimientos o bien cambios o nuevos controles para mitigar los incidentes de seguridad además de las mejoras en seguridad.

- *Cambios en los servicios de proveedores o socios comerciales para poner en práctica mejoras en los servicios de telecomunicaciones*, *uso de nuevas tecnologías, cambio de versiones de productos o nuevas versiones que surjan, nuevas herramientas de desarrollo y ambientes, cambios físicos e instalaciones, cambios de proveedores, socios comerciales y subcontratación de otros proveedores*, *en el tanto procedan legalmente.*

b) Los funcionarios y trabajadores que ejerzan como administradores de contratos deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o socios comerciales.

c) En los contratos o acuerdos con los proveedores o socios comerciales se deberá incluir una causal de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las políticas de seguridad de la información.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

5.23 Seguridad de la información para el uso de los servicios en la nube

La institución debe supervisar, revisar, evaluar y gestionar regularmente los cambios en las prácticas de seguridad de la información de los proveedores, socios comerciales y en la seguridad de información en los servicios de la nube, éstos deben establecerse de acuerdo con los requisitos de seguridad de la información de la institución, según lo especificado en el pliego de condiciones o en el contrato correspondiente. Es importante destacar que la seguridad en la nube es una responsabilidad compartida entre el proveedor de la nube y el cliente, según sea el caso.

Propósito

Especificar y gestionar la seguridad de la información para el uso de los servicios en la nube.

Orientación

La institución debe establecer y comunicar a las partes interesadas que corresponda las mejores prácticas en el uso de los servicios en la nube y cómo pretende gestionar los riesgos de seguridad de la información asociados a éste.

El uso de los servicios en la nube implica una responsabilidad compartida entre el proveedor de la nube y el cliente en materia de seguridad de la información y un esfuerzo de colaboración entre ambas partes. Por lo que es esencial que las responsabilidades tanto del proveedor de servicios en la nube como de la institución que actúa como cliente se definan y apliquen adecuadamente, como sigue:

a) Tomar decisiones de lo que se puede o no, migrar a la Nube, como: datos, servicios, aplicaciones, procesos, etc.

b) Realizar la evaluación del riesgo de los activos que van a ser movidos a la nube, teniendo presente un posible aumento de tráfico, operaciones y datos.

c) Identificar el valor de los activos en términos de confidencialidad, integridad, disponibilidad y el riesgo asociado al realizar la migración, ya sea de forma parcial o total, a la nube.

d) Si la institución lleva sus servicios a la nube, tercerizando diferentes tareas de la gestión de TI; nunca debe perder el control sobre la información y sobre la seguridad de ésta.

e) Antes de contratar este tipo de servicios es primordial evaluar las condiciones del servicio y las medidas de seguridad aplicadas; es decir, que las condiciones sean las adecuadas para garantizar el servicio y la protección de la información de la institución.

f) Se deberá valorar los escenarios de servicios en la nube, según su clasificación en infraestructuras públicas, privadas, comunitarias o híbridas; donde: a) con la nube pública la información está disponible para el público en general y dicha infraestructura la controla un proveedor de servicios en la nube, b) con la nube privada: la infraestructura de esta nube es operada únicamente por y para la institución, c) con la nube comunitaria la infraestructura de esta nube es compartida por varias organizaciones relacionadas entre ellas y que comparten requisitos de servicio, y d) en la nube híbrida es la combinación de dos o más modelos, por Ej. privada y pública, que permanecen como entidades únicas independientes pero que coexisten por tener tecnología que permite compartir datos o aplicaciones entre ellas.

g) Se deberá definir el modelo de servicio, entre: a) SaaS (Software as a Service). El proveedor del servicio es el encargado de ofrecer al cliente o a la entidad el software como un servicio, por Ej. las aplicaciones, servicio en entorno Web, las

aplicaciones de ofimáticas, etc., b) PaaS (Platform as a Service). El proveedor del servicio se encarga de entregar una plataforma al cliente. El cliente no administra ni controla la infraestructura, pero tiene el control sobre las aplicaciones instaladas y su configuración, y puede incluso instalar nuevas aplicaciones. c) IaaS (Infrastructure as a Service). El proveedor del servicio se encarga de entregar una infraestructura al cliente, normalmente mediante una plataforma de virtualización. El proveedor se encarga de la administración de la infraestructura y el cliente tiene el control sobre los sistemas operativos, almacenamiento y aplicaciones desplegadas, así como el control de los componentes de red virtualizados.

h) Observancia de la normativa de seguridad de la información en la nube para minimizar los riesgos a que se encuentran expuestos los activos de información, así como, prevenir un uso indebido y lograr el aprovechamiento eficiente de la infraestructura y servicios proporcionados en las redes y la nube.

i) Cumplir con los controles establecidos para regular los alcances de la prestación de servicios en la nube, es decir la definir responsabilidad compartida entre el cliente y proveedor.

j) Establecer claramente los roles y responsabilidades de seguridad de la información en la nube en el desempeño de las actividades. De igual forma, se deben establecer responsabilidades en la finalización de contrato o cambio de la relación laboral.

k) Establecer especificaciones para el sistema de gestión de claves, incluidos los procedimientos para cada proceso de ciclo de vida de la clave, es decir, generación, cambios, retiros, recuperar, retener y destruir; así como procedimientos de gestión de claves.

l) Se deberán definir las especificaciones del servicio relacionadas con las redes de transporte, incluida la capacidad de redes y la redundancia, para el servicio en la nube.

m) Se deberá monitorear el uso de los recursos del servicio y reconfigurarlos si es necesario para que se cumplan los requisitos respecto al rendimiento del sistema, así como proyectar los requisitos futuros de rendimiento del sistema para garantizar la disponibilidad de suficiente capacidad del servicio en la nube.

n) Apoyar la gestión de incidentes de seguridad de la información en la nube mediante herramientas de monitoreo de seguridad y detección, con el fin de evitar eventos relacionados con ataques y actividades maliciosas en los procesos, sistemas, redes y los servicios brindados, así como mantener el registro de los eventos que sirven como evidencia para sustentar los incidentes detectados, respaldar las acciones realizadas y las decisiones tomadas ante una eventualidad.

o) Establecer un plan de continuidad del negocio (PCN) para los servicios en la nube en el que se especifique como se desarrollarían los planes de recuperación ante desastres en caso de que se produzcan, qué mecanismos de copias de seguridad tienen, dónde se guarda esta información, sitios alternos distantes entre sí, redundancia y cuánto tiempo se tardaría en tener la solución completa al problema y tiempo de puesta en operación del servicio.

p) La implementación y el uso de la nube debe ser evaluada no sólo en el contexto "interno" y "externo", también, en lo que respecta a la ubicación física, los recursos, información, la legislación aplicable, y acuerdos contractuales, de igual forma, por quienes los están utilizando (tipo de usuario), así como por el responsable de su gestión, seguridad y cumplimiento a las políticas y estándares adoptados.

q) Mientras el servicio de nube se brinde por parte del ICE o bien el ICE sea usuario del servicio de nube, se deberán implementar controles técnicos, administrativos y físicos para mantener la confidencialidad, integridad y disponibilidad de los datos del ICE o del tercero al cual el ICE brinde el servicio de nube.

r) Se debe garantizar en el contrato respectivo, sin que represente costo adicional, la portabilidad total y posterior borrado de los datos en tránsito y en reposo o cualquiera que sea la modalidad de almacenamiento, todo lo anterior bajo la protección de datos personales, regulada en la Constitución Política, en la Ley Protección de las Personas frente al Tratamiento de los Datos Personales N° 8968 del 5 de noviembre de 2011, además, cuando así corresponda en base a la ubicación de la infraestructura, de la Regulación de Protección de Datos Generales de la Unión Europea (GDPR) del 25 de mayo de 2018, así como el Instituto Nacional de Estándares y Tecnologías (NIST) 800-53 referente al Control de Privacidad y Seguridad para Sistemas de Organización Federal y otras Organizaciones, y demás legislación o normativa aplicable, así como conforme con las mejores prácticas en la legislación de protección de datos.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

Código	Ley, Política, Norma
Ley 8968	Ley Protección de las Personas frente al Tratamiento de los Datos Personales.
GDPR	Regulación de Protección de Datos Generales de la Unión Europea.
(NIST) 800-53	Control de Privacidad y Seguridad para Sistemas de Organización Federal y Organizaciones.

5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información

La institución debe planificar y prepararse para gestionar los incidentes de seguridad de la información definiendo, estableciendo y comunicando los procesos de gestión de incidentes de seguridad de la información, las funciones y las responsabilidades.

Propósito

El propósito de estos lineamentos es definir claramente las funciones y responsabilidades del CSIRT para la investigación y respuesta de incidentes de seguridad informática y violaciones de datos.

Orientación

Este control se aplica a los sistemas de información, independientemente de su propiedad o ubicación, utilizados para almacenar, procesar, transmitir o acceder a los datos del ICE, así como a todo el personal, incluidos funcionarios, trabajadores, trabajadores temporales, contratistas, socios comerciales, empleados de entidades contratadas y otros autorizados para acceder a los activos del ICE y recursos de información relacionada.

Para esto se debe:

a) Establecer responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad.
b) Definir los objetivos para la gestión de incidentes de seguridad. Se deben acordar con la gerencia y garantizar, que los responsables de la gestión de incidentes de seguridad entiendan las prioridades de la institución para manejar los incidentes de seguridad.
c) Establecer objetivos de capacitación y entrenamiento para el personal encargado de la atención y gestión de incidentes.
d) Generar conciencia sobre temas tales como:

- Los beneficios de un enfoque formal y consistente para la gestión de incidentes (personal y organizacional).
- Cómo funciona el programa, expectativas.
- Cómo reportar Incidentes de Seguridad, a quién contactar.
- Restricciones impuestas por acuerdos de confidencialidad.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
SC.CDSE.021.2019	Lineamientos para la Atención de Incidentes de Seguridad de la Información y Ciberseguridad.
SC.CDSE.009.2019	Proceso de Manejo de Incidentes de Seguridad de la Información.
SC.CDSE.010.2019	Procedimiento Valoración y Ajuste a la Infraestructura.
SC.CDSE.011.2019	Procedimiento Detección y Análisis de Incidentes.
SC.CDSE.012.2019	Procedimiento Contención.
SC.CDSE.013.2019	Procedimiento Investigación de Incidentes de Seguridad de la Información.
SC.CDSE.014.2019	Procedimiento Erradicación de Incidentes de Seguridad.
SC.CDSE.015.2019	Procedimiento Recuperación de Incidentes de Seguridad de la Información.

5.25 Evaluación y decisión sobre eventos de seguridad de la información

La institución debe evaluar los eventos de seguridad de la información y decidir si deben ser categorizados como incidentes de seguridad de la información.

Propósito

Garantizar la categorización y priorización efectiva de los eventos de seguridad de la información.

Orientación

Debe acordarse un esquema de categorización y priorización de los incidentes de seguridad de la información para la identificación de las consecuencias y la prioridad de un incidente. El esquema debe incluir los criterios para categorizar los eventos como incidentes de seguridad de la información. El punto de contacto debe evaluar cada evento de seguridad de la información utilizando el esquema acordado.

Los eventos de la seguridad de la información pueden clasificarse en simples eventos o pueden pasar a ser incidentes de la seguridad de la información.

A efectos de valorizarlos correctamente, es necesario;

a) Un criterio de priorización de incidentes dependiendo del sistema o servicio afectado, del usuario, de la criticidad de la información o de cualquier otro elemento que intervenga en la priorización.

b) La evaluación de incidentes debe ser realizada tanto por el usuario como por el equipo de gestión que debe revisar la prioridad.

c) Llevar un registro de la evaluación de los incidentes para poder analizar los parámetros de calidad tanto en su resolución como de su clasificación.

Hay muchas formas de clasificar incidentes, pero lo habitual es considerar dos parámetros:

a) **Impacto:** Daño causado a la institución (en términos económicos, imagen, etc.).

b) **Urgencia:** La rapidez con la cual la institución necesita corregir el incidente.

La combinación de estos parámetros nos permitirá determinar la prioridad de cada incidente.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.

Código	Ley, Política, Norma
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
SC.CDSE.021.2019	Lineamientos para la Atención de Incidentes de Seguridad de la Información y Ciberseguridad.
SC.CDSE.009.2019	Proceso de Manejo de Incidentes de Seguridad de la Información.
SC.CDSE.010.2019	Procedimiento Valoración y Ajuste a la Infraestructura.
SC.CDSE.011.2019	Procedimiento Detección y Análisis de Incidentes.
SC.CDSE.012.2019	Procedimiento Contención.
SC.CDSE.013.2019	Procedimiento Investigación de Incidentes de Seguridad de la Información.
SC.CDSE.014.2019	Procedimiento Erradicación de Incidentes de Seguridad.
SC.CDSE.015.2019	Procedimiento Recuperación de Incidentes de Seguridad de la Información.

5.26 Respuesta a los incidentes de seguridad de la información

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

Propósito

Garantizar una respuesta eficiente y eficaz a los incidentes de seguridad de la información.

Orientación

La institución debe establecer y comunicar al personal los procedimientos de respuesta a los incidentes de seguridad de la información. Tratándose de proveedores y socios comerciales deberá incluirse en el pliego de condiciones o el contrato la obligación de rendir una declaración jurada en la que se comprometen a acatar la normativa interna en materia de seguridad de la información, incluidos estos procedimientos, a mantenerse actualizados de todas las modificaciones o reformas de las disposiciones o documentos normativos en la materia, incluidos los procedimientos, cuando se publiquen en el Diario

Oficial La Gaceta, en caso contrario (cuando no se publique en la Gaceta), el administrador del contrato, debe comunicárselas.

Se trata de controlar el proceso de resolución de incidentes en la seguridad de la información. Este control se aplica a los sistemas de información, independientemente de su propiedad o ubicación, utilizados para almacenar, procesar, transmitir o acceder a los datos del ICE, así como a todo el personal, incluidos funcionarios, trabajadores, trabajadores temporales, contratistas, socios comerciales, empleados de entidades contratadas y otros autorizados para acceder al ICE, activos de la empresa y recursos de información.

Los controles por establecer serian:

a) El Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) detecta e investiga eventos de seguridad para determinar si se ha producido un incidente y el alcance, la causa y el daño provocado.

b) El CSIRT dirige la recuperación, contención y remediación de incidentes de seguridad y puede autorizar y acelerar los cambios en los sistemas de información necesarios para hacerlo.

c) El CSIRT coordina la respuesta con partes externas cuando los acuerdos existentes asignan la responsabilidad de las investigaciones de incidentes a la parte externa.

d) Durante la realización de investigaciones de incidentes de seguridad, el CSIRT está autorizado a monitorear los recursos de TI del ICE relevantes y recuperar comunicaciones y otros registros relevantes de usuarios específicos de recursos de TI del ICE, incluidos los datos de sesión de inicio de sesión y el contenido de comunicaciones individuales sin previo aviso o aprobación adicional y en cumplimiento de los lineamientos establecidos para el monitoreo.

e) Cualquier divulgación externa de información relacionada con incidentes de seguridad de la información debe ser revisada y aprobada su envío por el Director de Ciberseguridad, el Gerente de Tecnología y Soluciones Digitales y el Gerente General en consulta con la División Jurídica, la Dirección de Comunicación y otras partes interesadas del ICE, según corresponda.

f) El CSIRT se coordina con las fuerzas del orden, las agencias gubernamentales, los CSIRT homólogos y los Centros de Análisis e Intercambio de Información (ISAC) relevantes en la identificación de incidentes de seguridad.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
SC.CDSE.021.2019	Lineamientos para la Atención de Incidentes de Seguridad de la Información y Ciberseguridad.
SC.CDSE.009.2019	Proceso de Manejo de Incidentes de Seguridad de la Información.
SC.CDSE.010.2019	Procedimiento Valoración y Ajuste a la Infraestructura.
SC.CDSE.011.2019	Procedimiento Detección y Análisis de Incidentes.
SC.CDSE.012.2019	Procedimiento Contención.
SC.CDSE.013.2019	Procedimiento Investigación de Incidentes de Seguridad de la Información.
SC.CDSE.014.2019	Procedimiento Erradicación de Incidentes de Seguridad.
SC.CDSE.015.2019	Procedimiento Recuperación de Incidentes de Seguridad de la Información.

5.27 Aprender de los incidentes de seguridad de la información

Los conocimientos adquiridos a partir de los incidentes de seguridad de la información deben utilizarse para reforzar y mejorar los controles de seguridad de la información.

Propósito

El propósito de este control es de contar con un registro fiable de conocimiento que permita realizar mejoras en la gestión de riesgos de información de la institución como consecuencia de incidentes experimentados.

Orientación

Este control se aplica a los sistemas de información, independientemente de su propiedad o ubicación, utilizados para almacenar, procesar, transmitir o acceder a los

datos del ICE, así como a todo el personal, incluidos funcionarios, trabajadores, trabajadores temporales, contratistas, socios comerciales, empleados de entidades contratadas y otros autorizados para acceder a los activos del ICE y recursos de información relacionados.

Para esto es requerido:

a) El conocimiento obtenido del análisis y la resolución de incidentes de seguridad debe utilizarse para reducir la probabilidad o el impacto de futuros incidentes.

b) Establecer reuniones de lecciones aprendidas para generar una sólida base de conocimientos ante futuros incidentes.

c) El CSIRT está autorizado a compartir información sobre incidentes y amenazas externas con las fuerzas del orden, las agencias gubernamentales, los CSIRT homólogos y los Centros de Análisis e Intercambio de Información (ISAC).

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
SC.CDSE.021.2019	Lineamientos para la Atención de Incidentes de Seguridad de la Información y Ciberseguridad.
SC.CDSE.009.2019	Proceso de Manejo de Incidentes de Seguridad de la Información.
SC.CDSE.010.2019	Procedimiento Valoración y Ajuste a la Infraestructura.
SC.CDSE.011.2019	Procedimiento Detección y Análisis de Incidentes.
SC.CDSE.012.2019	Procedimiento Contención.
SC.CDSE.013.2019	Procedimiento Investigación de Incidentes de Seguridad de la Información.
SC.CDSE.014.2019	Procedimiento Erradicación de Incidentes de Seguridad.
SC.CDSE.015.2019	Procedimiento Recuperación de Incidentes de Seguridad de la Información.

5.28 Recolección de evidencias

La institución debe establecer e implementar procedimientos para la identificación, recolección, adquisición y preservación de las pruebas relacionadas con los eventos de seguridad de la información.

Propósito

Garantizar una gestión coherente y eficaz de las pruebas relacionadas con los incidentes de seguridad de la información a efectos de fundamentar acciones disciplinarias y/o judiciales.

Orientación

Deben desarrollarse y seguirse procedimientos internos cuando se traten pruebas relacionadas con eventos de seguridad de la información a efectos de acciones disciplinarias y judiciales. Deben tenerse en cuenta los requisitos de las diferentes leyes, normas y reglamentaciones para maximizar las posibilidades de éxito de las acciones disciplinarias o judiciales que se presenten.

Los incidentes sobre la seguridad de la información pueden requerir decisiones posteriores como sanciones o acciones judiciales, por lo que recuperar las evidencias para utilizarlas posteriormente puede complicarse si no se tiene previsto algún mecanismo para guardarlas.

En este caso, la norma nos pone como control el que conservemos la información sobre las incidencias de forma que la podamos recuperar, al menos:

a) Los inicios y cierres de sesión.
b) Las identificaciones.
c) El estado de los dispositivos y de las redes.
d) Las evidencias de reuniones informativas, documentación sobre responsabilidades y funciones de seguridad del personal.

Se deben realizar análisis forenses de las evidencias informáticas para todos los casos y mantener los derechos de acceso a la información para poder resguardar la cadena de custodia.

Se requiere implementar procedimientos para el levantado y resguardo de evidencias tanto físicas como lógicas y contar con herramientas que aseguren la cadena de custodia.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.

Código	Ley, Política, Norma
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
SC.CDSE.021.2019	Lineamientos para la Atención de Incidentes de Seguridad de la Información y Ciberseguridad.
SC.CDSE.009.2019	Proceso de Manejo de Incidentes de Seguridad de la Información.
SC.CDSE.010.2019	Procedimiento Valoración y Ajuste a la Infraestructura.
SC.CDSE.011.2019	Procedimiento Detección y Análisis de Incidentes.
SC.CDSE.012.2019	Procedimiento Contención.
SC.CDSE.013.2019	Procedimiento Investigación de Incidentes de Seguridad de la Información.
SC.CDSE.014.2019	Procedimiento Erradicación de Incidentes de Seguridad.
SC.CDSE.015.2019	Procedimiento Recuperación de Incidentes de Seguridad de la Información.

5.29 Seguridad de la información durante la interrupción

La institución debe planificar cómo mantener la seguridad de la información en un nivel adecuado durante la interrupción de servicios.

Propósito

Garantizar la continuidad de la seguridad de la información del ICE, por medio de la implementación de acciones de recuperación establecidas, que permitan reaccionar ante eventos que impliquen una posible interrupción de sus procesos críticos o afectación a la confidencialidad, integridad y disponibilidad de la información.

Orientación

Los controles contenidos en este apartado pretenden contribuir a la protección de la información y de los activos que la trasiegan a nivel del ICE.

La institución debe determinar sus requisitos para adaptar los controles de seguridad de la información durante la interrupción. Los requisitos de seguridad de la información deben incluirse en los procesos de gestión de la continuidad del negocio.

Se debe desarrollar, implementar, probar, revisar y evaluar planes para mantener o restaurar la seguridad de la información de los procesos de negocio críticos tras una interrupción o un fallo. La seguridad de la información debe restablecerse al nivel y en los plazos requeridos.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

5.30 Preparación de las TIC para la continuidad del negocio

Las Tecnologías de Información y Comunicaciones (TIC) debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y de los requisitos de continuidad de las TIC así como ejercer el control respectivo.

Propósito

Garantizar la disponibilidad de la información de la institución y otros activos asociados durante la interrupción.

Orientación

La preparación de las TIC para la continuidad del negocio es un componente importante en la gestión de la continuidad del negocio y la gestión de la seguridad de la información para garantizar que los objetivos de la institución puedan seguir cumpliéndose durante la interrupción.

Los requisitos de continuidad de las TIC son el resultado del análisis de impacto empresarial (BIA). El proceso de BIA debe utilizar los tipos de impacto y los criterios para evaluar los impactos en el tiempo resultantes de la interrupción de las actividades de la institución que ofrecen productos y servicios. La magnitud y la duración del impacto resultante deberían utilizarse para identificar las actividades prioritarias a las que debería asignarse un objetivo de tiempo de recuperación (RTO). A continuación, el BIA debería determinar qué recursos son necesarios para apoyar las actividades priorizadas.

También debería especificarse un RTO para estos recursos. Un subconjunto de estos recursos debería incluir los servicios de TIC.

El BIA que incluye los servicios de TIC puede ampliarse para definir los requisitos de rendimiento y capacidad de los sistemas de TIC y los objetivos de punto de recuperación (RPO) de la información necesarios para apoyar las actividades durante la interrupción.

Sobre la base de los resultados del BIA y de la evaluación de riesgos que afectan a los servicios de las TIC, la institución debe identificar y seleccionar estrategias de continuidad de las TIC que consideren opciones para antes, durante y después de la interrupción. Las estrategias de continuidad del negocio pueden comprender una o más soluciones. Sobre la base de las estrategias, deben desarrollarse, implementarse y probarse planes para cumplir con el nivel de disponibilidad requerido de los servicios de TIC y en los plazos requeridos tras la interrupción o el fallo de los procesos críticos.

Por tanto, es necesario:

a) Identificar la infraestructura, los productos y servicios críticos, deben priorizarse según los niveles mínimos de entrega aceptables y el período máximo de tiempo que el servicio puede estar inactivo antes de que se produzcan daños graves en la institución.
b) Determinar la clasificación de la infraestructura, productos y servicios críticos, para determinar el impacto de una interrupción en la prestación de servicios, pérdida de ingresos, gastos adicionales y pérdidas intangibles.
c) Determinar cuánto tiempo podría funcionar la institución sin la infraestructura, producto o servicio crítico ante una interrupción. Y cuánto tiempo los clientes aceptarían su falta de disponibilidad. Será necesario determinar el período de tiempo en que un producto o servicio podría no estar disponible antes de que se sienta un impacto severo.
d) Determinar qué procesos y funciones que respaldan la prestación de infraestructura, productos y servicios están involucrados en la generación de ingresos.
e) Identificar las pérdidas intangibles para determinar el costo aproximado de la pérdida de confianza de los clientes, daños a la reputación o imagen, pérdida de competitividad, reducción de la participación en el mercado y violación de las leyes y reglamentos.
f) Analizar y revisar constantemente las capacidades de recuperación actuales y considerar las soluciones de recuperación que la institución ya tiene establecidas y su aplicabilidad continua mediante un proceso de mejora continua.

g) Conformar equipos de comando y control que incluyen un equipo de gestión de crisis, gestión de seguridad de la información, gestión de seguridad informática y continuación o recuperación.

h) Establecer y documentar los deberes y responsabilidades para cada equipo e incluir la identificación de los miembros del equipo y la estructura de autoridad, identificación de las tareas específicas de cada equipo, los roles y responsabilidades de los miembros, creación de listas de contactos, fijación de posibles miembros alternativos.

i) Establecer medidas y controles para que los equipos funcionen a pesar de la pérdida o indisponibilidad de personal, por ejemplo, puede ser necesario que cada miembro de equipo deba realizar tareas múltiples y brindar capacitación entre equipos.

j) Asegurar que los sitios alternativos cuenten con las características de seguridad que minimizan el impacto de las interrupciones. Entre otras, teniendo en cuenta la suficiente distancia entre el sitio principal y el sitio alterno.

k) Los planes de continuidad del negocio deben implementarse de manera fluida y efectiva mediante la información adecuada a todos los funcionarios o trabajadores sobre el contenido del plan y de sus responsabilidades individuales.

l) Tener funcionarios o trabajadores con responsabilidades directas capacitados para las tareas que deberán realizar, y estar al tanto de las funciones de otros equipos.

m) Después de la capacitación, se deben desarrollar y programar ejercicios para lograr y mantener altos niveles de competencia y preparación como método para validar el plan.

n) Ajustar las estrategias de seguridad de la información, planear y justificar las inversiones en tecnología, personal y programas que cubran posibles vectores de ataque.

o) Garantizar la disponibilidad y correcta asignación de recursos para mitigar los errores de seguridad de la información identificados.

p) Aumentar el conocimiento en seguridad del personal interno desarrollando un programa específico basado en hechos, que cubran los vectores de ataque relevantes.

q) Identificar cuáles son las categorías de amenazas que más impacto tienen y qué tipo de información vulnera para defenderse de ellas.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

5.31 Requisitos legales, reglamentarios y contractuales

Los requisitos legales, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben ser identificados, documentados y mantenidos al día.

Propósito

Garantizar el cumplimiento de cualquier ley, regulación u obligación contractual relacionada con el uso y manejo de los activos de información correspondientes con la gestión del ICE.

Orientación

Es requerido identificar los requisitos legales, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la institución para cumplir con estos requisitos deben ser identificados, documentados y mantenidos al día.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

5.32 Derechos de propiedad intelectual

La institución debe aplicar procedimientos adecuados para proteger los derechos de propiedad intelectual.

Propósito

Cumplir con los requisitos de legislación nacional, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos patentados.

Orientación

De acuerdo con la “Política de Propiedad Intelectual e Industrial del Grupo ICE”, es necesario considerar los siguientes controles con el fin de proteger cualquier material que pueda considerarse propiedad intelectual:

a) Todos los funcionarios, trabajadores y/o proveedores deben acatar lo establecido en la *“Política de Propiedad Intelectual e Industrial del Grupo ICE”*.

b) Las dependencias deberán solicitar la consultoría y/o acompañamiento del Proceso Seguridad de la Información de la Dirección Ciberseguridad, GTSD, con el fin implementar los controles de seguridad de la información que propicien la protección de la información relacionada con secretos comerciales e industriales, declarada confidencial, persona jurídica o física, para las creaciones e invenciones (por ejemplo: obras artísticas, literarias, software, marcas de servicio o de productos, signos distintivos, nombres comerciales, señales de propaganda, emblemas, secretos industriales, patentes de invención, modelos de utilidad y diseños industriales, entre otros).

c) Suscribir acuerdos de confidencialidad con los funcionarios, trabajadores o terceros cuando se crean productos, servicios e invenciones.

d) Todo documento que contenga cláusulas de confidencialidad deberá ser revisado previamente por el Proceso Soporte a la Gestión Empresarial de la GTSD y el Proceso Seguridad de la Información cuando corresponda.

e) Las dependencias deberán garantizar que los secretos comerciales, industriales, o económicos cuenten con los mecanismos y requisitos necesarios para controlar uso, manejo y/o transferencia.

f) Las dependencias deberán comunicar y concientizar a los funcionarios, trabajadores y terceros, acerca de la *“Política de Propiedad Intelectual e Industrial del Grupo ICE”* y sus posibles consecuencias en caso de una infracción a la propiedad intelectual y seguridad de la información.

g) Se deben identificar, documentar y actualizar para cada sistema de información y para la Institución todos los requisitos legales, reglamentarios y contractuales atinentes a la seguridad de la información; de forma tal que se asegure los

derechos de propiedad intelectual (tanto de desarrollos internos como de propiedad intelectual de terceros), protección de registros sensibles contra pérdida, destrucción, falsificación, acceso no autorizado y la divulgación no autorizada; y la privacidad y protección de datos personales de los clientes.

h) Se deberá contar con un consentimiento escrito por parte de un representante del ICE, debidamente facultado para tal efecto, para el uso de sus productos intelectuales e industriales, por parte de los funcionarios, trabajadores, socios comerciales, aliados o terceros.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
35.00.001.2010	Política de Propiedad Intelectual e Industrial del Grupo ICE.

5.33 Protección de los registros

Los registros deben estar protegidos contra la pérdida, la destrucción, la falsificación, el acceso no autorizado y la divulgación no autorizada.

Propósito

Garantizar el cumplimiento de cualquier ley, regulación u obligación contractual relacionada con el uso y manejo de los activos de información correspondientes con la operación del ICE. Es importante tener identificados todos los requerimientos legales, contractuales o regulatorios que sean aplicables a la gestión del ICE para garantizar su cumplimiento.

Orientación

Los controles contenidos en este apartado pretenden contribuir a la protección de la información y de los activos que la trasiegan a nivel del ICE.

Cada dependencia que implemente un Sistema de Gestión de Seguridad de la Información, deberá asignar un responsable de la Gestión Documental, quien se encargue de llevar el adecuado control de los registros documentales del SGSI.

El gestor documental debe realizar el mantenimiento del sistema de documentación de la dependencia, esto según el plan de trabajo definido y las prioridades establecidas en cumplimiento de las recomendaciones surgidas en las revisiones del SGSI. Este rol, debe realizar el seguimiento y comprobación de que la documentación está conforme a lo establecido en el SGSI. Además, debe realizar las revisiones periódicas de la documentación, actualizarla y custodiarla.

A continuación de indican los controles generales para efectos del manejo de los registros de información:

1. La elaboración o modificación de un formato de registro deberá tramitarse por medio del Procedimiento de Elaboración y el Control de Documentos con que disponga a donde se realice dicha acción. Los registros deben contener: el nombre y/o firma de quien lo completa o actualiza, fecha de cuando se completó o actualizó.
2. El titular subordinado debe registrar y mantener actualizada la lista de registros vigentes relacionados con el sistema de gestión de seguridad.
3. Todos los documentos del sistema de gestión de seguridad de la información que den origen a formatos para registros o que hagan referencia a un registro de origen externo contarán con una sección en forma de tabla, en la cual se definan los requisitos específicos para cada uno de los formatos internos o externos tal y como se indica a continuación:
    a. **Código y nombre del registro:** en dicha columna se indicará el código y el nombre del registro. Para los registros de origen externo se indicará, cuando sea aplicable, el código y nombre.
    b. **Ubicación del respaldo:** se debe indicar la dirección electrónica o física (si aplica) donde se respalda el registro.
    c. **Acceso Autorizado:** en dicha columna se indicará o funcionario (s) o trabajador (es) que tienen acceso autorizado al documento o registro.
    d. **Versión:** se debe indicar la versión en la cual fue elaborado el documento.
    e. **Control de cambios:** Este se indicará en el apartado “Control de cambios” que tiene cada documento formalizado.
    f. **Tiempo de conservación:** en dicha columna se indicará el tiempo durante el cual se conservará el registro antes de su descarte o eliminación.

g. **Retención y disposición:** en cada documento se incluye un apartado de "Control de registros" donde se indica el tiempo de retención del documento y la disposición que tendrá cuando el mismo ya no sea utilizado.

Una vez aprobado el nuevo formato de registro se desechan las versiones anteriores.

En el caso que no sea aprobado el nuevo formato se deberá volver a elaborar o modificar para su aprobación.

4. Para el mantenimiento de los registros electrónicos del sistema, el responsable del registro debe realizar el respaldo electrónico, por orden cronológico el cual es colocado en un sitio colaborativo o carpeta compartida.

   El tiempo de almacenamiento de un registro debe establecerse para cada caso, según lo disponga, tomando en cuenta las leyes, los reglamentos y demás normativa que aplique.

   Al finalizar el tiempo de almacenamiento o tiempo de conservación previsto, el titular subordinado a cargo o quien este delegue, procederán a descartar los documentos que ya no se utilizarán más, esto se hará en conjunto con el Proceso Gestión de Documentación Institucional (GEDI).

   En caso de que se considere necesario, la dependencia que implemente un sistema de gestión de seguridad de la información deberá establecer un procedimiento para realizar el control de registros y establecer los mecanismos necesarios para la adecuada protección de éstos.

Derechos de propiedad intelectual relacionados con uso de software

Se debe aplicar los controles para asegurar el cumplimiento de las leyes, regulaciones y aspectos contractuales para el manejo los derechos de propiedad intelectual y sobre el uso de los productos de "*software"* en los servicios de información dentro del ICE.

Todo "*software"* instalado en los equipos tecnológicos del ICE debe estar de acuerdo con las disposiciones de la "Ley de Procedimientos de Observancia de los Derechos de Propiedad Intelectual. Nº 8039".

La Dirección Soluciones Tecnológicas de la Gerencia Tecnología y Soluciones Digitales, debe supervisar el apego al uso de licencias y cumplimiento con los derechos de autor de toda aplicación y herramienta de "*software"* utilizada en las estaciones de trabajo, para el monitoreo y configuración de la infraestructura tecnológica del ICE.

Protección de datos personales

Debe garantizarse la protección de datos personales de funcionarios, trabajadores, clientes, proveedores, socios comerciales y cualquier otra persona involucrada con el ICE, según legislación y normativa vigente, Ley Protección de la Persona frente al Tratamiento de sus Datos Personales N° 8968 y su respectivo reglamento.

Revisiones de seguridad de la información

Se debe aplicar los controles para asegurar que el procesamiento de la información y los sistemas involucrados cumplen con las políticas y estándares de seguridad definidos dentro de la Política Empresarial de Seguridad de la Información.

La Gerencia Tecnología y Soluciones Digitales y el Proceso Gestión de Documentación Institucional (GDI), deben definir o proponer según corresponda las pautas a seguir para establecer mecanismos para el resguardo y respaldo de la información, según la normativa vigente, las regulaciones de la industria y las mejores prácticas; así mismo mantenerse en apego de los lineamientos o procedimientos establecidos con tal finalidad.

Generales:

a) Los activos de información serán resguardados según lo definido en la tabla de plazos por los responsables de la información, en coordinación con el Proceso Gestión Documental Institucional y la Dirección Soluciones Tecnológicas de la GTSD.
b) El Proceso Gestión Documental Institucional, en conjunto con los responsables de la información, elaborarán una tabla de plazos, donde se definen los tiempos requeridos para la conservación de los activos de información.
c) Los respaldos serán revisados aleatoriamente por los responsables de la información.
d) Se debe procurar que la ejecución de los respaldos no altere la operación normal de los sistemas.

Cumplimiento con las políticas y normas de seguridad

Se deben implementar mecanismos para verificar el cumplimiento de los requisitos de seguridad de la información contenidos en este documento. En caso de que se detecte un incumplimiento es requerido identificar la causa que lo origina, tomar medidas para corregirlo, realzar acciones para implementar esas medidas y por último verificar que las acciones tomadas sean efectivas.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
ISO 27001:2022	Apartado 8.1.2 Propiedad de los Activos.
19.00.001.2017	Lineamientos para el Funcionamiento del Modelo de Arquitectura de Información Empresarial para el Grupo ICE.
76.00.001.2016	Procedimiento para la Actualización del Modelo de Objetos y Datos a Nivel Conceptual.
48.00.001.2017	Procedimiento para la Actualización del Tesauro Especializado en Electricidad y Telecomunicaciones.
Ley 7202	Ley del Sistema Nacional de Archivos.
Decreto Ejecutivo 40554	Reglamento a la Ley del Sistema Nacional de Archivos.
48.00.007.2010	Manual para el Funcionamiento del Modelo Archivístico Institucional.
Ley 8039	Ley de Procedimientos de Observancia de los Derechos de Propiedad Intelectual.
Ley 8968	Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales.

5.34 Privacidad y protección de la información personal

La institución debe identificar y cumplir los requisitos relativos a la preservación de la privacidad y protección de la Información de Identificación Personal (IIP), de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales.

Propósito

Garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales asociados con los términos de seguridad de la información para la protección de la IIP.

Orientación

La institución debe establecer y comunicar al personal, una normativa que contemple aspectos sobre privacidad y protección de la información sensible.

Tratándose de proveedores y socios comerciales deberá incluirse en el pliego de condiciones o el contrato la obligación de rendir una declaración jurada en la que se comprometen a acatar la normativa interna en materia de seguridad de la información, a mantenerse actualizados de todas las modificaciones o reformas de las disposiciones o documentos normativos en la materia, incluido estos lineamientos, cuando se publiquen en el Diario Oficial La Gaceta, en caso contrario (cuando no se publique en la Gaceta), el administrador del contrato, debe comunicárselas. En la materia se establecen las siguientes obligaciones:

a) *Toda persona física que deba facilitar a la Institución el acceso a datos personales deberá firmar un consentimiento para ello, de conformidad con la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, N° 8968.*
b) *El almacenamiento de toda IIP se debe realizar acorde a lo estipulado en la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, N° 8968.*

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
Ley 8968	Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales.

5.35 Revisión independiente de la seguridad de la información

El enfoque de la institución para la gestión de la seguridad de la información y su aplicación, incluyendo a las personas, los procesos y las tecnologías, debe revisarse de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.

Propósito

Garantizar la idoneidad, adecuación y eficacia del enfoque y las medidas que se han implementado en la institución para gestionar la seguridad de la información.

Orientación

La institución debe generar un proceso en el que se incluyan las revisiones independientes, tales como las siguientes:

a) El titular subordinado debe tener un proceso establecido en el que se tengan planificadas las revisiones independientes de forma periódica.

b) Las revisiones o auditorías se realizarán para verificar el cumplimiento de objetivos, controles, políticas y procedimientos de seguridad de la información, además, deben considerarse dentro de las evaluaciones, las oportunidades de mejora y establecer así mismo la necesidad de realizar cambios o acciones correctivas.

c) Las revisiones serán ejecutadas por personal independiente de la dependencia revisada y deberán poseer las competencias adecuadas para realizarlo.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

5.36 Cumplimiento de las políticas, reglas y normas de seguridad de la información

El cumplimiento de toda la normativa relacionada con la Seguridad de la Información de la institución, deben revisarse regularmente.

Propósito

Garantizar que la seguridad de la información se aplique y funcione de acuerdo con la Política Empresarial de Seguridad de la Información de la institución, la Política Corporativa de Ciberseguridad, y los demás documentos normativos que regulen el tema.

Orientación

Establecer, revisar e implementar la normativa interna de seguridad de la información necesaria con el fin de cumplir con la legislación vigente, los requisitos contractuales y estándares internacionales adoptados por la Institución en materia de seguridad de la información.

La principal función del Proceso Seguridad de la Información es ser un aliado estratégico de la Empresa para establecer criterios de seguridad de la información. En ese sentido, se utilizará metodologías para clasificar la información, diagnósticos de seguridad, gestión de riesgos y revisión de cumplimiento de la seguridad de la información.

La Dirección Ciberseguridad realizará revisiones de cumplimiento de la normativa de seguridad de la información. Estas revisiones deberán ser coordinadas y planificadas para minimizar el riesgo de interrupciones en la empresa.

La Dirección Ciberseguridad en conjunto con las dependencias competentes determinará los requerimientos de revisiones de cumplimiento, cuyo alcance será acordado y controlado por todo el personal involucrado.

Para ello se debe:

- Permitir a los funcionarios y trabajadores el acceso mínimo necesario para desempeñar sus labores.
- Los Gerentes, jefes de división, directores y coordinadores, como dueños de los procesos establecidos, deben apoyar las revisiones del cumplimiento de las políticas de seguridad de la información que les competa y cualquier otro requerimiento de seguridad.
- Acatar en todos sus extremos la “Política Corporativa de Confidencialidad de la Información” mediante la implementación de controles y protocolos de seguridad para el resguardo de la información declarada confidencial en virtud del artículo 35 de la Ley de Fortalecimiento de las Entidades Públicas del Sector de Telecomunicaciones N° 8660, así como de información de los clientes, usuarios de los servicios y cualquier otra información que por disposición constitucional o legal sea de naturaleza confidencial.
- Acatar en todos sus extremos la Política de Transparencia y Revelación de Información del Grupo ICE.

- Promover una cultura de seguridad de la información, mediante comunicados, capacitaciones y acciones de seguimiento y mejora en las dependencias de la Institución.
- Establecer los mecanismos jurídicos necesarios para salvaguardar el uso de la información Institucional en la gestión con terceros, y la información suministrada por los clientes en virtud de los servicios. Los mecanismos jurídicos serán coordinados entre la División Jurídica y la Dirección Ciberseguridad, según lo amerite cada caso.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.
38.00.002.2019	Política de Transparencia y Revelación de Información del Grupo ICE.
Ley 8660	Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector de Telecomunicaciones.

5.37 Procedimientos operativos documentados

Los procedimientos operativos de las instalaciones de procesamiento de la información deben documentarse y ponerse a disposición del personal que los necesite.

Propósito

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información dentro del ICE.

Orientación

Los controles contenidos en este apartado pretenden contribuir a la protección de la información y de los activos que la trasiegan a nivel del ICE.

a) Los procedimientos de operación son documentados por cada área Técnica del ICE en coordinación con los Procesos Soporte a la Gestión de la Gerencia correspondiente, con el fin de garantizar que se dé un adecuado manejo y clasificación de la información, además de estandarizar los documentos y evitar duplicados y retrabajo innecesario.

b) La documentación será custodiada por el gestor documental, bajo la guía del Administrador del SGSI, con el fin de garantizar que haya una adecuada revisión y actualización de los documentos.

c) Los coordinadores de cada área deben de facilitar un sitio colaborativo, donde la documentación esté actualizada y formalizada, con el fin de que el personal pueda acceder a la última versión actualizada y aprobada.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

6 CONTROLES DE PERSONAS

6.1 Proyección

Las comprobaciones de los antecedentes de todos los candidatos a convertirse en personal deben llevarse a cabo antes de su incorporación a la institución y de forma continuada, teniendo en cuenta las leyes, los reglamentos y la ética aplicables, y ser proporcionales a los requisitos del negocio, la clasificación de la información a la que se va a acceder y los riesgos percibidos.

Propósito

El personal elegible debe ser el idóneo para las funciones para las que se le considera, condición debe mantenerse durante la relación laboral.

Orientación

Realizar, cuando corresponda, procesos de selección para todo el personal, sea temporal, parcial o tiempo completo, y cuando sea una contratación por medio de un proveedor de servicios, deben incluirse los requisitos de selección en las condiciones de la contratación.

Si las funciones para las cuales se contratará a la persona son relativas a Seguridad de la Información, la institución deberá:

a) Asegurar que el individuo posee las competencias para ejercer una función de Seguridad de la Información.
b) Realizar revisiones de seguridad detalladas adicionales, con criterios y limitaciones establecidas.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
Art. 7 Sesión 5817-2007 Consejo Directivo	Estatuto de Personal.
32.00.003.2015	Reglamento Autónomo Laboral.
RRS.001.2006	Reglamento de Reclutamiento, Evaluación y Selección de Personal.
OPN 32.PSI.001.2006	Procedimiento para el Reclutamiento y Selección Interna.
32.00.003.2011	Procedimiento para la Contratación de Servicios Especiales.
32.01.001.2007	Procedimiento para la Creación de Plazas Nuevas.

6.2 Condiciones de empleo

Los acuerdos contractuales de empleo deben establecer las responsabilidades del personal y de la institución en materia de seguridad de la información.

Propósito

Garantizar que el personal entienda sus responsabilidades en materia de seguridad de la información para las funciones para las que se le considera.

Orientación

Las obligaciones a las que se encuentra sujeto el personal deben considerar la normativa asociada a Seguridad de la Información de la institución y mejores prácticas.

Para tal efecto:

a) La institución debe asegurarse que los funcionarios y trabajadores entiendan sus responsabilidades y sean aptos para los roles para los cuales están siendo considerados.

b) El ICE cuenta con un área rectora en recursos humanos para realizar estas labores, la cual se encarga de realizar el proceso de investigación del personal a contratar.

c) Las funciones y tareas de cada puesto de trabajo estarán establecidas en los perfiles de puesto; por lo que las responsabilidades y la formación en materia de seguridad deben ir acordes a éstos, sea esta inicial o complementaria según sean las necesidades.

d) El ICE cuenta con documentos normativos con referencia a la selección y contratación de recursos humanos.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

Código	Ley, Política, Norma
Art. 7 Sesión 5817-2007 Consejo Directivo	Estatuto de Personal.
32.00.003.2015	Reglamento Autónomo Laboral.
RRS.001.2006	Reglamento de Reclutamiento, Evaluación y Selección de Personal.
OPN 32.PSI.001.2006	Procedimiento para el Reclutamiento y Selección Interna.
32.00.003.2011	Procedimiento para la Contratación de Servicios Especiales.
32.01.001.2007	Procedimiento para la Creación de Plazas Nuevas.
32.01.007.2009	Procedimiento para la Aplicación de Exámenes Médicos de Ingreso.
24.00.001.2005	Proceso de Selección Externa de Personal.
32.01.006.2009	Procedimiento para la Calificación Final del Trabajador.

6.3 Concientización, educación y formación en materia de seguridad de la información

El personal de la institución debe recibir una concientización, educación y formación adecuadas en materia de seguridad de la información, así como las actualizaciones periódicas de la Política Empresarial de Seguridad de la Información y de la Política Corporativa de Ciberseguridad, así como de la normativa específica de este tema específico, según corresponda a su función laboral o contractual. Esta comunicación la deberá realizar el área responsable de la política según aplique.

Tratándose de proveedores o socios deberá incluirse en el pliego de condiciones o el contrato la obligación de rendir una declaración jurada en la que se comprometen a capacitar a su personal en materia de seguridad de la información.

Propósito

Garantizar que el personal y las partes interesadas pertinentes conozcan y cumplan sus responsabilidades en materia de seguridad de la información.

Orientación

Debe establecerse un programa de concientización, educación y formación en materia de seguridad de la información en consonancia con la Política Empresarial de Seguridad de la Información, los documentos normativos de temáticas relacionadas y los procedimientos pertinentes en materia de seguridad de la información, teniendo en cuenta la información de la institución que debe protegerse y los controles de seguridad de la información que se han aplicado para ese fin.

La concientización, la educación y la formación en materia de seguridad de la información debe realizarse periódicamente. La concientización, educación y formación iniciales pueden aplicarse al personal nuevo y a los que se trasladan a nuevos puestos de trabajo o ante cambios en sus funciones con requisitos de seguridad de la información sustancialmente diferentes.

La comprensión del personal debe evaluarse al final de una actividad de sensibilización, educación o formación para comprobar la transferencia de conocimientos y la eficacia del programa de sensibilización, educación y formación.

Para ejecutar esas acciones se requiere:

a) Desarrollar documentos, campañas de información, etc. adecuados para la concientización en materia de seguridad, controles, protección de equipos desatendidos, así como de sus responsabilidades, leyes y normativa, dirigido a funcionarios, trabajadores y partes interesadas pertinentes.

b) Efectuar actividades de concientización e instrucción a los funcionarios y trabajadores, diseñadas para propiciar la comprensión de los procesos de continuidad las operaciones y garantizar que los procesos sigan siendo eficaces.

c) Elaborar un plan de capacitación y concientización dirigido a los funcionarios y trabajadores identificados como los activos intelectuales (Know-How, secretos industriales, conocimiento sobre las operaciones críticas, etc.), dado la importancia que revisten éstos para el cumplimento de los objetivos estratégicos de la institución, tomando en cuenta los riesgos a los que están expuestos.

d) Concientizar a los funcionarios y trabajadores para que conozcan los riesgos y la manera como ellos pueden ayudar a la institución a evitar pérdidas reportando oportunamente las anomalías que identifiquen.

e) Efectuar capacitación especializada, para los funcionarios y trabajadores que son parte de los procesos de seguridad de la información y seguridad informática con el fin de tener bases más sólidas no solo para conocer sobre seguridad, sino para trabajar y aplicar sus conocimientos en el día a día.

f) Asegurar que los funcionarios y trabajadores desde el principiante hasta el más experimentado tengan los conocimientos suficientes para desempeñar eficientemente sus funciones.

g) El plan de concientización sobre la seguridad de la información debe ser sometido a actualización constante referente a las nuevas tecnologías y los retos de seguridad que se va dando día a día.

h) Tener en cuenta un mejoramiento continuo, debido al avance de la tecnología, nuevas amenazas, vulnerabilidades, nuevas formas de atacar por parte de los cibercriminales, actualizaciones de las normas o estándares que impactan en la Política Empresarial de Seguridad de la Información.

i) Enfocar el plan de concientización y capacitación no solo en procesos, dispositivos, herramientas y tecnologías, sino en quienes definen los procesos, las personas, que son el principal actor que debe educarse, formarse y adquirir una cultura en Seguridad de la Información, ellos tienen el primer contacto con los datos y la información del cliente.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

6.4 Proceso disciplinario

Para conseguir la correcta implementación de la Política Empresarial de Seguridad de la Información y toda la normativa asociada a la temática, se aplicará el procedimiento disciplinario formal al personal que vulnere o la normativa de seguridad de la información.

Propósito

Garantizar que las consecuencias del incumplimiento de la normativa de Seguridad de la Información sean comprendidas por el personal.

Orientación

Las faltas y las eventuales sanciones asociadas al incumplimiento de la normativa de Seguridad de la Información serán establecidas institucionalmente por los órganos competentes.

Se debe concientizar al personal sobre las consecuencias del incumplimiento de la normativa de seguridad de la información.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
DARH-POD-PRO-001	Procedimiento Ordinario Disciplinario.
32.01.001.2009	Procedimiento para la Solicitud de Medidas Cautelares.
32.SC.008.2006	Procedimiento para Pagos de Liquidaciones Externos.
32.01.006.2009	Procedimiento para la Calificación Final del Trabajador(a)
Art. 7 Sesión 5817-2007 Consejo Directivo	Estatuto de Personal.
32.00.003.2015	Reglamento Autónomo Laboral.
RRS.001.2006	Reglamento de Reclutamiento, Evaluación y Selección de Personal.
OPN 32.PSI.001.2006	Procedimiento para el Reclutamiento y Selección Interna.
32.00.003.2011	Procedimiento para la Contratación de Servicios Especiales.
32.01.001.2007	Procedimiento para la Creación de Plazas Nuevas.

6.5 Responsabilidades tras la terminación o el cambio de empleo

Las responsabilidades y los deberes en materia de seguridad de la información se mantienen tras el cese de la relación laboral, el cambio de funciones o finalización de la relación laboral, y deben definirse, aplicarse y comunicarse al personal pertinente y a otras partes interesadas, según corresponda.

Propósito

El objetivo de este control es conseguir que aquellos usuarios que cesen las relaciones con la institución lo hagan de forma que la información a la que tenían acceso no sea amenazada con posterioridad a la finalización de la relación, con independencia del tipo de ésta, sea laboral, contractual o de acceso.

Orientación

Debe gestionarse un proceso para la finalización o el cambio de empleo en el que se definirán responsabilidades y deberes en materia de seguridad de la información, los cuales deben seguir vigentes después de la terminación o el cambio.

Gestiones como las siguientes:

a) La dependencia en la cual se desempeñaba el funcionario o trabajador debe comunicar la finalización del empleo a otras dependencias con las que estuviera involucrado el empleado, para poder realizar las tareas necesarias como cambios en las labores, transferencia de conocimientos y eliminación de accesos.

b) Incluir en el contrato o acuerdo previo, las responsabilidades que deben ser válidas después de la finalización de un contrato o el cambio de empleo.

c) Los deberes y responsabilidades en materia de seguridad de la información de cualquier persona o funcionario que cambie de puesto de trabajo deben ser identificadas y transferidas a otra persona.

d) Dentro del proceso deben incluirse los terceros o proveedores cuando finalicen los contratos que posean con la institución.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

Código	Ley, Política, Norma
Art. 7 Sesión 5817-2007 Consejo Directivo	Estatuto de Personal.
32.00.003.2015	Reglamento Autónomo Laboral.
RRS.001.2006	Reglamento de Reclutamiento, Evaluación y Selección de Personal.
OPN 32.PSI.001.2006	Procedimiento para el Reclutamiento y Selección Interna.
32.00.003.2011	Procedimiento para la Contratación de Servicios Especiales.
32.01.001.2007	Procedimiento para la Creación de Plazas Nuevas.

6.6 Acuerdos de confidencialidad o de no divulgación

Deben aplicarse medidas de seguridad para el personal o terceros que gestionan información, para proteger la información a la que se accede, se procesa o se almacena.

Propósito

Garantizar la seguridad de la información cuando el personal o terceros gestionan información (presencial, teletrabajo, lugar de trabajo flexible, entornos de trabajo virtuales, entre otros).

Orientación

Asegurar la confidencialidad, acceso y gestión de la información del ICE.

A continuación, se detalla:

a) Solicitar al Proceso Seguridad de la Información y al Proceso Soporte Gestión Empresarial respectivo, la consultoría para la elaboración de los acuerdos de confidencialidad, según se requiera que contenga la importancia del resguardo y gestión adecuada de la información, las responsabilidades bajo de los funcionarios y/o terceros, para tal fin es necesario que las dependencias recopilen y brinden la información necesaria para dicho acuerdo.

b) Las dependencias deberán identificar las necesidades de firma de un acuerdo de confidencialidad con el funcionario, trabajador o terceros, para ello es necesario confeccionar el documento en coordinación con la División Jurídica y/o el Proceso Seguridad de la Información y custodiar dichos contratos de confidencialidad firmados en el expediente de personal correspondiente o el de la contratación o

acuerdo comercial. El acuerdo debe indicar claramente al trabajador parte interesada según corresponda, los alcances y consecuencias del acuerdo a suscribir.

c) Solicitar al Proceso Seguridad de la Información, la asesoría de acuerdo con el marco jurídico nacional referente al manejo de los diferentes contratos de información confidencial que son administrados en el ICE, aclaración de consultas y ejecución de las acciones requeridas en caso de que le sea notificado un incumplimiento técnico. En caso de ser necesario Seguridad de la Información elevará a la División Jurídica lo que corresponda.

d) El Proceso Seguridad de la Información deberá brindar respuesta ante las consultas de naturaleza técnica de confidencialidad que realicen las dependencias. En caso de tratarse de consultas jurídicas las respuestas serán brindadas por la División Jurídica según corresponda.

e) Las dependencias deberán identificar las necesidades de firma de un acuerdo de confidencialidad con el trabajador o terceros, para ello es necesario confeccionar el documento en coordinación con el Proceso Seguridad de la Información y custodiar dichos contratos de confidencialidad firmados en el expediente de personal correspondiente.

f) Definir y comunicar acerca de las responsabilidades alineadas a su competencia y su gestión adecuada con la información confidencial o privada.

g) Los funcionarios, trabajadores o terceros deberán firmar y cumplir conforme a lo establecido en el acuerdo de confidencialidad.

h) Una vez finalizada la relación laboral con el ICE, deberá permanecer el deber de confidencialidad, por lo que la divulgación no autorizada de información confidencial puede generar responsabilidad.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
Ley 7975	Ley de Información no Divulgada.

6.7 Trabajo remoto

Deben aplicarse medidas de seguridad cuando el personal ICE o de terceros, trabaja a distancia para proteger la información a la que se accede, se procesa o se almacena fuera de las instalaciones de la institución.

Propósito

Preservar la seguridad de la información cuando el personal del ICE o de terceros trabaje en modalidad virtual o a distancia.

Orientación

El trabajo a distancia o teletrabajo se realiza cuando el personal trabaja desde un sitio fuera de las instalaciones de la institución, teniendo acceso a la información empresarial, ya sea en papel o por un medio electrónico.

Para ello, debe revisar los siguientes puntos:

a) Generar una normativa que abarque los términos y condiciones que deban cumplirse para la modalidad de teletrabajo; en la institución se cuenta con el *Reglamento para la Aplicación del Teletrabajo en el ICE código* 32.00.009.2008, el cual contempla los controles técnicos y administrativos necesarios para optar por el programa de teletrabajo dentro de la institución.

b) El manejo de información empresarial mediante dispositivos móviles debe realizarse conforme al Reglamento para la Utilización de la Información del ICE mediante Dispositivos Móviles 87.00.001.2022.

c) La normativa debe considerar a funcionarios, trabajadores, proveedores, socios comerciales, que requieran acceder a servicios o información del ICE por medio de dispositivos externos.

d) Las medidas de seguridad física que se implementen estarán orientadas a la prevención de daños, hurtos o extravíos de los equipos portátiles.

e) Es responsabilidad del usuario la aplicación de estas medidas y de la jefatura correspondiente el girar las instrucciones para el acatamiento de estas pautas.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.

Código	Ley, Política, Norma
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
87.00.001.2022	Reglamento para la Utilización de la Información del ICE mediante Dispositivos Móviles.
32.00.009.2008	Reglamento para la Aplicación del Teletrabajo en el ICE.

6.8 Informes de eventos de seguridad de la información

La institución debe proporcionar un mecanismo para que el personal y los usuarios informen por medio de canales apropiados y de manera oportuna, los eventos de seguridad de la información observados o sospechosos.

Propósito

Apoyar la notificación oportuna, coherente y eficaz de los eventos de seguridad de la información que puedan ser identificados por el personal o cualquier usuario.

Orientación

El personal de la Institución o el usuario tienen la obligación de reportar al Grupo de Respuesta a Incidentes de Seguridad de la Información (CSIRT), cualquier actividad sospechosa de seguridad de la información, con el fin de que se determine si corresponde a un incidente de seguridad de la información y se le brinde el tratamiento establecido. La inobservancia de esta obligación puede acarrear responsabilidad disciplinaria y de otra índole de acuerdo con la gravedad de la omisión por parte del trabajador.

La Dirección Ciberseguridad, establecerá una metodología para la gestión de incidentes de seguridad de la información empresarial, que permita gestionar y responder todos los incidentes de seguridad de la información que se presentan tanto a lo interno como en los servicios que se brindan a los clientes.

La Dirección Ciberseguridad, en conjunto con otras dependencias competentes, coordinará las acciones para gestionar, propiciar y asesorar la respuesta a todo incidente de seguridad que afecte la confidencialidad, integridad y disponibilidad de la información empresarial.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.

7 CONTROLES FÍSICOS

7.1 Perímetros de seguridad física

Los perímetros de seguridad deberán ser definidos y utilizados para proteger las áreas que contienen información y otros activos asociados.

Propósito

Evitar el acceso físico no autorizado, los daños y las interferencias en la información de la institución y otros activos asociados.

Orientación

Establecer los requerimientos de negocio frente al control de acceso. Limitar el acceso a las instalaciones de procesamiento de información y garantizar los accesos de usuarios autorizados e impedir los accesos no autorizados a los sistemas de información.

Impedir el acceso de usuarios no autorizados y el compromiso o robo de información y recursos para el tratamiento de la información, así como prevenir el acceso no autorizado a los sistemas y aplicaciones de los activos estratégicos del ICE.

El ICE contará con perímetros físicamente sólidos para los edificios o sitios que contengan instalaciones de procesamiento de información crítica. Las paredes, techos y suelos exteriores de los recintos deben ser de construcción sólida y todas las puertas exteriores deben estar convenientemente protegidas contra el acceso no autorizado con mecanismos de control (por ejemplo, barras, alarmas, cerraduras). Las puertas y ventanas deberán estar cerradas con llave cuando estén desatendidas y deberán

considerarse la posibilidad de instalar una protección externa en las ventanas, sobre todo a nivel del suelo; también deberán tenerse en cuenta los puntos de ventilación.

Alarmar, supervisar y probar todas en un perímetro de seguridad junto con las paredes para establecer el nivel de resistencia requerido de acuerdo con las normas adecuadas, funcionando a prueba de fallos.

La protección física puede lograrse creando una o más barreras físicas alrededor de los locales de la institución y de las instalaciones de procesamiento de la información.

Una zona segura puede ser una oficina con cerradura o varias salas rodeadas por una barrera de seguridad física interna continua. Pueden ser necesarias barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requisitos de seguridad dentro del perímetro de seguridad. El ICE deberá considerar la posibilidad de contar con medidas de seguridad física que puedan reforzarse en situaciones de mayor amenaza.

Conceptualmente el dispositivo de seguridad aplicable a las instalaciones críticas en el ICE está basado en el modelo de cerrado-cerrado. Es decir, es una instalación que permanentemente se mantiene cerrada al ingreso de personas y puede ser accedida únicamente en condiciones específicas de autorización.

Para estos casos por ejemplo se cumplen los siguientes requisitos:

a) El perímetro de seguridad está claramente definido y representado en un croquis donde se pueden apreciar los perímetros, las áreas seguras y los principales activos protegidos.
b) El perímetro del edificio en el que están ubicados activos críticos de información tiene solidez física y todas las puertas están convenientemente protegidas contra accesos no autorizados al disponerse de un equipo de oficiales de seguridad, un sistema de control de movimiento y un circuito cerrado de televisión.
c) En el interior de las instalaciones se dispone de un sistema de alarma que detecta accesos no autorizados en las zonas de trabajo.
d) El acceso tanto al recinto como a cada una de las zonas de este requiere de la identificación previa de todas las personas.
e) El dispositivo de seguridad (por defecto) está basado en tres subsistemas articulados a saber:
    - **Seguridad Operativa:** Conjunto de personas que han sido asignadas para la aplicación de procedimientos y la ejecución de acciones preventivas y de respuesta ante eventos que atenten contra la integridad de los intereses que han sido puestos bajo su responsabilidad.

- **Seguridad Física:** Se trata de todas aquellas barreras o medios de carácter constructivo o geológico que puedan ser instaladas o aprovechadas para la mejor protección de las instalaciones y la minimización de riesgos y amenazas.
- **Seguridad Electrónica:** Aprovechamiento de los desarrollos tecnológicos en los medios de protección. Se subdivide en: · Circuito cerrado de televisión (CCTV) · Sistema de control de acceso · Sistema de detección de intrusión · Sistema de alarmas y aviso.

f) Estas instalaciones deben tener muros perimetrales con sensores de aproximación, dichos muros fueron construidos con el propósito de proteger las instalaciones. La instalación estará sectorizada en tres grandes áreas de trabajo ubicadas en forma de anillos concéntricos iniciando desde afuera hacia el interior, considerando los diversos niveles de seguridad y el tipo de amenazas que afronta desde cada punto de evaluación.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

7.2 Entrada física

Las zonas seguras deberán estar protegidas por controles de entrada y puntos de acceso adecuados.

Propósito

Garantizar que sólo se produce el acceso físico autorizado a la información de la institución y a otros activos asociados.

Orientación

Los puntos de acceso, como las zonas de entrega y carga y otros puntos en los que pueden entrar personas no autorizadas, deberán estar controlados y, si es posible, aislados de las instalaciones de procesamiento de la información para evitar el acceso no autorizado.

Las zonas seguras deberán estar protegidas por controles de entrada y puntos de acceso adecuados, implementado las siguientes acciones:

a) El ICE establecerá las normas de actuación y revisión a seguir por parte de los Oficiales de Seguridad ubicados en los Puestos de Seguridad del ICE con la finalidad de prevenir situaciones de riesgos y amenazas, así como controlarlas y canalizarlas en caso de presentarse. Aplica para todas las personas que transiten (ingreso y salida) por los Puestos de Seguridad del ICE.

b) Las normas indicadas en el punto anterior tienen por objeto establecer los parámetros de actuación para el otorgamiento de autorizaciones de acceso a cualquiera de las instalaciones críticas del ICE en el país y a las personas que por motivos válidos requieran ingresar a ellas.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
10.00.002.2009	Reglamento para el Uso de Carné Corporativo de las Empresas del Grupo ICE.
10.00.001.2009	Reglamento General de Acceso y Tránsito a Instalaciones del Instituto Costarricense de Electricidad.

7.3 Asegurar las oficinas, salas e instalaciones

Se debe diseñar e implementar la seguridad física de las oficinas, salas e instalaciones.

Propósito

Impedir el acceso físico no autorizado, los daños y las interferencias en la información de la institución y otros activos asociados en oficinas, salas e instalaciones.

Orientación

Para asegurar las oficinas, las salas y las instalaciones el ICE cuenta con las siguientes reglas:

a) Ubicar las instalaciones críticas para evitar el acceso no autorizado.
b) Cuando proceda, garantizar que los edificios sean discretos y den una indicación mínima de su propósito, sin señales obvias, fuera o dentro del edificio, que identifiquen la presencia de actividades de procesamiento de información.
c) Configurar las instalaciones para evitar que la información o las actividades confidenciales sean visibles y audibles desde el exterior. También debe considerarse el blindaje electromagnético, según proceda.
d) La ubicación, mediante cualquier medio, de las instalaciones que son utilizadas para el resguardo o procesamiento de información confidencial, no deben ser accesibles a personas no autorizadas.

Con base en lo anterior, se cuentan con controles de ingreso como, por ejemplo; la presentación de la identificación o carné, la autorización de ingreso, identificación biométrica como la huella digital o la anotación en bitácora.

Para tomar en cuenta aspectos de manejo de emergencias, se debe poner en práctica simulacros para realizar evacuación del personal en caso de que se presentara un evento, bajo coordinación con el Centro Coordinador de Operaciones de Emergencias (CCOE).

Además, en el interior de las instalaciones se debe de contar con mapas donde se indican las rutas de salida o evacuación a seguirse por parte del personal y los visitantes.

Se deben seguir las normas de seguridad establecidas en los protocolos de seguridad física.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
10.00.002.2009	Reglamento para el Uso de Carné Corporativo de las Empresas del Grupo ICE.
10.00.001.2009	Reglamento General de Acceso y Tránsito a Instalaciones del Instituto Costarricense de Electricidad.

7.4 Vigilancia de la seguridad física

Las instalaciones deben estar continuamente vigilados para evitar el acceso físico no autorizado.

Propósito

Detectar e impedir el acceso físico no autorizado.

Orientación

Las instalaciones físicas deben ser supervisadas por sistemas de vigilancia, que pueden incluir oficiales de seguridad, alarmas contra intrusos, sistemas de vigilancia por vídeo, como la televisión de circuito cerrado, y programas informáticos de gestión de la información sobre seguridad física, ya sean gestionados internamente o por un proveedor de servicios de vigilancia.

Seguridad Electrónica: Aprovechamiento de los desarrollos tecnológicos en los medios de protección. Se subdivide en: · Circuito cerrado de televisión (CCTV) · Sistema de control de acceso · Sistema de detección de intrusión · Sistema de alarmas y aviso. La vigilancia y control a través de la seguridad física se lleva a cabo con el fin de proteger un espacio determinado para evitar daños y minimizar amenazas.

Es imprescindible identificar los posibles riesgos y amenazas que hay en el lugar y buscar los elementos físicos que se requieran para suministrar una excelente protección.

La seguridad física tiene como finalidad prevenir, disminuir, detener o disuadir los atentados o amenazas que puedan afectar la seguridad de nuestros clientes o de sus bienes más preciados mediante la utilización de sistemas y de personal idóneo en seguridad para la vigilancia y control.

Algunas de las amenazas que se pueden minimizar o evitar con los elementos de la seguridad física, son los incendios, robos, homicidios, secuestros, suplantación y robo de información, los cuales se analizan y se identifican según la probabilidad de amenaza (altamente probable, probable, poco probable y probabilidad desconocida).

Cualquier mecanismo de monitoreo y grabación debe ser utilizado teniendo en cuenta las leyes y reglamentos vigentes, incluida la legislación sobre protección de datos y de la información personal, especialmente en lo que respecta a la supervisión del personal y a los períodos de conservación de los vídeos grabados.

El Proceso Seguridad Informática, de la Dirección Ciberseguridad de la Gerencia Tecnología y Soluciones Digitales, es la dependencia encargada del diseño, instalación, operación y mantenimiento de los sistemas de seguridad electrónica ubicados en las instalaciones físicas del ICE.

Incidentes de seguridad electrónica:

El Proceso Seguridad Informática debe llevar a cabo un plan de trabajo anual, en donde se atiendan los sistemas de seguridad electrónica del ICE.

El Proceso Seguridad Informática realizará el mantenimiento preventivo y correctivo de los sistemas de la seguridad electrónica.

El citado Proceso también debe atender de forma oportuna los incidentes relacionados con dichos sistemas que están dedicados a la preservación de las instalaciones.

Incidentes de seguridad física:

El Proceso Gestión Seguridad Institucional, de la Gerencia Servicios y Recursos Empresariales, tendrá a cargo las labores de protección mediante la disposición de Oficiales de Seguridad, destinados exclusivamente para las instalaciones del ICE.

El Proceso Gestión Seguridad Institucional debe contar con procedimientos de control y vigilancia para la protección de las personas y bienes, mediante la prevención, detección, alerta o mitigación de alguna situación, sea por eventos de origen delictivo, accidental o natural, que comprometa la integridad de los dispositivos de protección física, los activos de la empresa, la operación normal de ésta, o también a las personas e imagen institucional.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
10.00.002.2009	Reglamento para el Uso de Carné Corporativo de las Empresas del Grupo ICE.
10.00.001.2009	Reglamento General de Acceso y Tránsito a Instalaciones del Instituto Costarricense de Electricidad.
SC.CAE.001.2019	Procedimiento para la Atención de los Mantenimientos Preventivos y Correctivos de los Equipos y Sistemas de Seguridad Electrónica.

Código	Ley, Política, Norma
SC.CAE.002.2019	Procedimiento para el Diseño de los Servicios de Seguridad Electrónica.
SC.CAE.003.2019	Procedimiento para el Desarrollo de Soluciones de los Equipos y Sistemas de Seguridad Electrónica.

7.5 Protección contra las amenazas físicas y medioambientales

La seguridad física y del entorno del ICE son todas las medidas tomadas para proteger los sistemas, los edificios y la infraestructura de apoyo relacionada contra las amenazas asociadas con el ambiente físico.

El ICE debe implementar, controlar y diseñar la protección contra las amenazas físicas y medioambientales, como los desastres naturales y otras amenazas físicas intencionadas o no intencionadas a la infraestructura.

Propósito

Prevenir o reducir las consecuencias de los eventos originados por las amenazas físicas y medioambientales.

Orientación

El ICE llevará a cabo evaluaciones de riesgo para identificar las consecuencias potenciales de las amenazas físicas y ambientales, las cuales, deben realizarse antes de comenzar las operaciones críticas en un sitio físico, y a intervalos regulares, aplicando las salvaguardias necesarias y supervisarse los cambios en las amenazas.

Para ello se debe obtener el asesoramiento de especialistas de Seguridad de la Información sobre cómo gestionar los riesgos derivados de las amenazas físicas y medioambientales, como; incendios, inundaciones, terremotos, explosiones, disturbios civiles, residuos tóxicos, emisiones medioambientales y otras formas de catástrofes naturales o provocadas por el ser humano.

Protección contra amenazas externas e internas:

El ICE asigna y aplica protección física contra daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre.

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

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

a) Los materiales peligrosos o combustibles deben ser almacenados a una distancia segura de la dependencia asegurada.
b) Los suministros a granel como papelería no deben almacenarse en la dependencia asegurada.
c) El equipo de reemplazo y los medios de respaldo deben ubicarse a una distancia segura para evitar el daño de un desastre que afecte el local principal.
d) La edificación destinada para el almacenamiento de la información, ciberseguridad y protección de la privacidad debe contar con los requerimientos básicos contra incendio para brindar una adecuada protección en caso de que se presente una emergencia.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
10.00.002.2009	Reglamento para el Uso de Carné Corporativo de las Empresas del Grupo ICE.
10.00.001.2009	Reglamento General de Acceso y Tránsito a Instalaciones del Instituto Costarricense de Electricidad.
Ley 8228	Ley del Benemérito Cuerpo de Bomberos de Costa Rica.
Ley 8488	Ley Nacional de Emergencias y Prevención del Riesgo.

7.6 Trabajar en zonas seguras

Deben diseñarse y aplicarse medidas de seguridad para trabajar en zonas seguras.

Propósito

Proteger la información y otros activos asociados en áreas seguras contra daños e interferencias no autorizadas por parte del personal que trabaja en estas áreas.

Orientación

Las medidas de seguridad para trabajar en zonas seguras se aplican a todo el personal y abarca todas las actividades que tengan lugar en ellas.

Para ello, el ICE diseña y aplica medidas de seguridad para trabajar en zonas seguras:

a) Haciendo que el personal sólo conozca la existencia de una zona segura o las actividades que se realizan en ella en función de la necesidad de conocerla.
b) Evitando el trabajo sin supervisión en zonas seguras, tanto por razones de seguridad como para reducir las posibilidades de actividades maliciosas.
c) Cerrando físicamente e inspeccionando periódicamente las zonas seguras vacías.
d) No permitiendo equipos de fotografía, vídeo, audio u otros equipos de grabación, como cámaras en los dispositivos de los usuarios, a menos que se autorice;
e) Controlando adecuadamente el transporte y el uso de los dispositivos de los usuarios en las zonas seguras.

Se cuenta con controles de ingreso por medio de la identificación o carné, la autorización de ingreso y/o del registro que se puede realizar por medio de huella digital o por anotación en bitácora.

Para tomar en cuenta aspectos de manejo de emergencias, el ICE ha de desarrollar un plan de Emergencias, el cual se practica para realizar evacuación del personal en caso de que se presentara un evento.

Además, en el interior del ICE se cuenta con mapas donde se indican las rutas de salida o evacuación a seguirse por parte del personal y los visitantes.

Se deben seguir las normas de seguridad establecidas en los protocolos de seguridad física de clientes, proveedores, funcionarios y trabajadores, respectivamente. Se deben colocar los procedimientos de emergencia en un lugar fácilmente visible o accesible.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.

Código	Ley, Política, Norma
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
10.00.002.2009	Reglamento para el Uso de Carné Corporativo de las Empresas del Grupo ICE.
10.00.001.2009	Reglamento General de Acceso y Tránsito a Instalaciones del Instituto Costarricense de Electricidad.

7.7 Escritorio y pantalla despejados

Deben definirse y aplicarse adecuadamente normas claras para los papeles y los medios de almacenamiento extraíbles y normas claras para las pantallas de las instalaciones de procesamiento de la información.

Propósito

Reducir los riesgos de acceso no autorizado, pérdida y daño de la información en los escritorios, pantallas y en otros lugares accesibles durante y fuera del horario de trabajo.

Orientación

Establecer y comunicar la normativa específica sobre el tema de la mesa de trabajo y la pantalla clara. Definir y aplicar adecuadamente normas claras para los papeles y los medios de almacenamiento extraíbles y normas claras para las pantallas de las instalaciones de procesamiento de la información.

El objetivo primordial es determinar las reglas para evitar el acceso no autorizado a la información en los puestos de trabajo, asimismo, a las instalaciones y equipos compartidos.

Los usuarios de los sistemas de información y comunicaciones del ICE deben bloquear la pantalla de su computador, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.

Los usuarios de los sistemas de información y comunicaciones del ICE deben cerrar las aplicaciones y servicios de red cuando no los necesite.

Equipo desatendido por el usuario

- En el ICE los usuarios de equipos deben dejarlos protegidos con contraseña cada vez que se retiran.
- Definir reglas para evitar el acceso no autorizado a la información en los puestos de trabajo, como también a las instalaciones y a los equipos compartidos. Toda la información clasificada como Información Sensible.

Lineamiento de escritorio limpio

- Si la persona autorizada no se encuentra en su puesto de trabajo, todos los documentos impresos, como también los soportes de almacenamiento de datos, etiquetados como sensibles, deben ser retirados del escritorio o de otros lugares (impresoras, equipos de fax, fotocopiadoras, etc.) para evitar el acceso no autorizado.
- Este tipo de documentos y soportes deben ser archivados de forma segura, de acuerdo con lo establecido en las buenas prácticas comúnmente aceptadas en el ámbito de Seguridad de la Información a nivel internacional.

Lineamiento de pantalla limpia

- Si la persona autorizada no se encuentra en su puesto de trabajo, se debe quitar toda la información sensible de la pantalla, y se debe denegar el acceso a todos los sistemas para los cuales la persona tiene autorización.
- En el caso de una ausencia corta (hasta 30 minutos), el lineamiento de pantalla limpia se implementa finalizando la sesión en todos los sistemas o bloqueando la pantalla con una clave. Si la persona se ausenta por un período más prolongado (superior a 30 minutos), el lineamiento de pantalla limpia se implementa finalizando la sesión en todos los sistemas y apagando el puesto de trabajo.

Protección de instalaciones y equipos compartidos.

- Los documentos que contienen información sensible deben ser retirados inmediatamente de las impresoras, fotocopiadoras y equipos de fax.
- Los discos virtuales donde el personal tiene acceso en común se protegen mediante el uso de usuario y contraseña, esto para evitar que otros no autorizados puedan ingresar a la documentación, solamente el personal de la dependencia que la jefatura disponga tendrá acceso a la información.
- Las impresoras que se utilicen deben estar protegidas por el uso de clave o código personal (PIN), con el fin de que sólo la persona que envió a imprimir los documentos pueda liberar la impresión y así evitar la exposición de información a otros.

- El uso no autorizado de impresoras, fotocopiadoras, escáneres y demás equipamiento compartido para copiado (equipo multifuncional ubicado en la Mesa de servicio) se evita mediante el uso de carné de acceso y huella (acceso biométrico).

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.
ISO 27001:2022	Apartado 8.1.2 Propiedad de los Activos.
19.00.001.2017	Lineamientos para el Funcionamiento del Modelo de Arquitectura de Información Empresarial para el Grupo ICE.

7.8 Ubicación y protección del equipo

Los equipos deben estar ubicados de forma segura y protegida.

Propósito

Reducir los riesgos derivados de las amenazas físicas y ambientales, y de los accesos y daños no autorizados.

Orientación

Proteger los equipos que procesan información de los negocios del ICE y especialmente los que contienen información de carácter confidencial para minimizar el riesgo de fuga de información de cualquier forma posible.

El personal de la institución debe cumplir con los controles establecidos para la ubicación y protección de los equipos considerando que todos los dispositivos deben estar protegidos, incluyendo aquellos que operen de manera desatendida.

La ubicación de los equipos debe realizarse de forma que reduzca las amenazas, peligros ambientales y oportunidades de acceso sin autorización.

El objetivo de la protección física de los equipos es contra un posible robo, acceso sin autorización, daño, manipulación no autorizada, incendios, inundaciones y cualquier otra actividad que ponga en riesgo la seguridad de la información empresarial.

La dependencia responsable de gestionar los incidentes de seguridad deberá estar capacitada para detectar y atender cualquier emergencia relacionada a la seguridad física que se presente en los equipos y contar con las herramientas y procedimientos necesarios para este fin.

El responsable de la dependencia de operación y mantenimiento de infraestructuras dispone de un inventario actualizado de los equipos que realizan un tratamiento y almacenamiento de la información, así como de las infraestructuras necesarias para la prestación del servicio.

La tipología de este inventario se debe alinear con lo contemplado en el análisis de riesgos, que se actualiza anualmente.

Periódicamente (al menos una vez al año), el responsable de la dependencia de operación y mantenimiento de infraestructuras (Redes, Electromecánica y TI) revisa el estado, número de serie, especificación y ubicación de los equipos de los clientes en los racks comprobando que el inventario se mantenga actualizado y que en caso de que haya habido una baja no contemplada o se ha sacado un equipo sin autorización, se actualice dicho inventario, o incluso en caso de que el equipo ha sido sustraído o retirado sin ser anotado en los formularios de los clientes.

Instalación y ubicación física

Todos los equipos que se utilicen en el ICE deben instalarse en zonas de manera que se minimicen los accesos innecesarios a las áreas de trabajo. Para el caso concreto de equipos que se utilicen para el tratamiento y almacenamiento de información considerada de importancia alta (según los resultados del análisis de riesgos) deben ser instalados donde sean reducidos los riesgos de que otros vean los procesos durante su uso.

Si los equipos requieren protección especial, se aislarán del resto para reducir el nivel general de protección requerido. En este sentido, los gabinetes que albergan servidores y equipos de comunicaciones deberán estar en todo momento cerrados con llave.

A partir de los resultados obtenidos en la identificación y análisis de riesgos, se establecen controles y medidas de seguridad para minimizar las posibles amenazas como el robo, incendio, humo o vibraciones, tal y como queda reflejado en el plan de tratamiento de riesgos.

Antes de la llegada de un equipo a las instalaciones del ICE, el responsable de la dependencia o la persona en quién éste delegue como responsable de acompañamiento, estudiará la ubicación del nuevo equipo para cumplir con las especificaciones descritas.

Servicios de suministro

Los equipos deben estar protegidos contra fallos de energía u otras anomalías eléctricas mediante un sistema complementario. Por un lado, existen una serie de generadores eléctricos que entrarían en funcionamiento en caso de fallo en el suministro de energía, por otro lado, existe un sistema de alimentación ininterrumpida (SAI) que permiten la continuidad de los sistemas hasta que entren en funcionamiento los generadores.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.
ISO 27001:2022	Apartado 8.1.2 Propiedad de los Activos.

7.9 Seguridad de los activos fuera de las instalaciones

Se debe proteger los activos fuera de las instalaciones.

Propósito

Evitar la pérdida, el daño, el robo o el compromiso de los dispositivos fuera de las instalaciones y la interrupción de las operaciones de la institución.

Orientación

Cualquier dispositivo utilizado fuera de las instalaciones de la institución que almacene o procese información (por ejemplo, un dispositivo móvil), incluidos los dispositivos de propiedad de la institución y los dispositivos de propiedad privada utilizados en nombre de la institución (BYOD bring your own device), necesita la respectiva protección.

Se debe aplicar seguridad al equipo fuera de las instalaciones del ICE tomando en cuenta los diferentes riesgos de trabajar fuera del local de la institución. Sin importar la propiedad, el uso de cualquier equipo de procesamiento de la información fuera del local del ICE debería ser autorizado por la jefatura y la GTSD.

Se deberán considerar los siguientes controles para la protección del equipo fuera del local:

a) El equipo y medios sacados del local nunca debería ser dejados desatendidos en lugares públicos; durante un viaje, las computadoras portátiles deberían ser llevadas como equipaje de mano y cuando sea posible, de manera disimulada.

b) Se debe observar en todo momento las instrucciones de los fabricantes para proteger el equipo; por ejemplo, protección contra la exposición a fuertes campos electromagnéticos.

c) Se debe determinar controles para el trabajo en casa a través de una evaluación del riesgo y los controles apropiados conforme sea apropiado; por ejemplo, archivos con llave, lineamiento de escritorio limpio, controles de acceso para las computadoras y una comunicación segura con la oficina.

En caso de salida de equipos de las instalaciones el oficial de seguridad revisará que los equipos a retirarse y sus respectivas series, hayan sido anotados en el formulario respectivo de control de ingreso y salida de herramientas, materiales, equipos, dispositivos, repuestos y vehículos.

En caso de que el equipo no esté indicado en el formulario, éste no podrá ser retirado de las instalaciones. En caso de que lo considere necesario, puede coordinar su salida en una futura visita.

El oficial de seguridad ejecutará la revisión a la salida de equipos de acuerdo con el formulario de control de ingreso y salida de herramientas, materiales, equipos, dispositivos, repuestos y vehículo.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

Código	Ley, Política, Norma
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.
ISO 27001:2022	Apartado 8.1.2 Propiedad de los Activos.

7.10 Medios de almacenamiento

Los soportes de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la institución.

Propósito

Garantizar sólo la divulgación, modificación, eliminación o destrucción autorizada de la información en los medios de almacenamiento.

Orientación

Con la implementación de procedimientos para la reutilización o eliminación segura de los medios de almacenamiento se minimiza el riesgo de filtración de información confidencial a personas no autorizadas. Los procedimientos para la reutilización o eliminación segura de los medios de almacenamiento que contienen información confidencial son proporcionales a la sensibilidad de dicha información.

El responsable de los activos de información, especialmente cuando se trata de información confidencial, y de infraestructura crítica, debe garantizar la seguridad durante su ciclo de vida, es decir, desde su creación hasta su eliminación, implementando las mejores prácticas.

Todos los activos de información producidos, generados o creados por los funcionarios o trabajadores en sus labores cotidianas, es información que pertenece a la institución y tiene los derechos de disposición y patrimonial sobre ésta y podrá utilizarla, como así lo requiera y se lo permita la ley. No así los funcionarios o trabajadores, quienes no podrán disponer de dichos activos de información para efectos no relacionados con sus labores cotidianas, a menos que cuenten con autorización válidamente emitida y por escrito, para ello, siempre que sean utilizados para el quehacer de la institución.

Los gestores de los activos de información deben seguir estrictamente todos los procedimientos y mecanismos aprobados por la institución para garantizar el adecuado procesamiento y el correcto almacenamiento de los datos.

Es obligación de todo funcionario o trabajador, reportar por los medios y canales seguros provistos por la institución, cualquier situación que pudiese comprometer la

confidencialidad, integridad y disponibilidad, así como la exactitud, fidelidad y veracidad de los activos de información que están bajo su custodia.

Cada funcionario o trabajador tendrá la obligación inexcusable de salvaguardar y proteger los datos personales y demás información confidencial a la tenga conocimiento en virtud de su relación con la institución. Todo activo de información referente a datos personales deberá ser tratada como información confidencial y no divulgarse.

La institución debe gestionar el acceso y uso de los diferentes medios de almacenamiento para mantener la confidencialidad, integridad y disponibilidad de los activos de información de la institución, para el control de la disposición final, habilitación, uso y des habilitación de acceso a éstos. También, identificar y autorizar los funcionarios y trabajadores que pueden, en el ejercicio de sus actividades laborales, conocer, actualizar, modificar y eliminar los activos de información que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por parte de la institución.

Todos los usuarios deben tener bloqueados los accesos a puertos USB, o medios de almacenamiento externos o memorias USB, las excepciones deben ser avaladas exclusivamente por los directores de cada área, según corresponda mediante nota interna a seguridad informática de la GTSD y se limitarán a los requerimientos del negocio, minimizando el riesgo respectivo siempre bajo el principio de la asignación de los mínimos privilegios posibles.

Establecer el grado de frecuencia y realizar copias de seguridad de los activos de información, con base en la criticidad de los activos de información implicados.

Los medios de respaldo y el procedimiento de restauración se deben ejecutarse según el plan de continuidad del negocio con regularidad, para garantizar la disponibilidad de los activos de información de forma oportuna ante posibles incidentes.

Establecer el método de borrado con base en la clasificación de los activos de información, teniendo en cuenta que los comandos de borrado del sistema operativo solo acceden a la «lista de archivos» y marcan el archivo como suprimido, pero su contenido permanece intacto. Y en cuanto al formateo de un dispositivo normalmente se sobrescribe el área destinada a la «lista de archivos» sin que el área de datos donde se encuentra el contenido de los archivos haya sido alterada.

La institución debe establecer métodos eficaces que eviten completamente la recuperación de los datos contenidos en los medios de almacenamiento, por ejemplo, la desmagnetización (potente campo magnético), la destrucción física (Desintegración, pulverización e incineración) y la sobre escritura en la totalidad de la superficie de almacenamiento (escritura de un patrón de datos modificando los valores almacenados).

Para el traslado de los medios de almacenamiento a otras instalaciones internas o externas de la institución, hay que asegurar y documentar que se cumple la cadena de custodia de éstos, para evitar fugas de información; de igual forma se debe aplicar para la eliminación de los activos de información.

Al seleccionar un método o herramienta de borrado, elegir aquella que permita la obtención de un documento que identifique claramente que el proceso de borrado se ha realizado, detallando cuándo, cómo ha sido realizado y por quién.

En el caso de que la destrucción lógica no se realice correctamente por fallo del dispositivo, este hecho deberá documentarse claramente y utilizar métodos de destrucción física de dicho soporte, asegurando que se realice de forma respetuosa con el medio ambiente según lo estable la institución.

Cuando un medio de almacenamiento se encuentre dañado, y la eliminación lógica de la información no sea posible, se debe realizar la destrucción física del dispositivo.

Disposición segura o reutilización de equipos

Su objetivo es garantizar que la información almacenada en equipos y soportes sea borrada o eliminada de forma segura.

Todos los datos y software con licencia almacenado en soportes móviles (por ej., CD, DVD, unidades USB, tarjetas de memoria, etc., y también en papel) y en todos los equipos que tienen soportes de almacenaje (por ej., ordenadores, teléfonos móviles, etc.) deben ser borrados, o se debe destruir el soporte, antes de ser eliminados o reutilizados.

Los responsables de los activos de información y de activos de soporte, deberán documentar lo actuado y asegurarse que, antes de eliminar o reutilizar un equipo (ya sean servidores, equipos de comunicaciones u ordenadores personales) por otra persona diferente a la habitual, la información contenida en el mismo haya sido borrada con la función normalizada de borrado (WIPE) o destruida físicamente; siempre y cuando esta información no sea necesaria para la prestación del servicio, de ser necesario coordinará con CSUF o Seguridad Informática de la GRSDT según corresponda.

Previamente el Comité del SGSI comprobará, antes de la eliminación de activos de información o de la reutilización de un equipo, que todos los elementos del equipo que contengan soportes de datos se hayan borrado o sobrescrito, mediante el respaldo documental de la dependencia que realizó la eliminación garantizando que se utilizó el procedimiento de borrado o eliminación correspondiente.

Los coordinadores de TI de las dependencias correspondientes son los responsables de verificar y borrar datos de los equipos. Los datos deben ser borrados mediante la forma que se considere más conveniente y segura, pero sí, teniendo en cuenta la sensibilidad de los datos, si el proceso no es suficientemente seguro, entonces los soportes de

almacenaje deben ser destruidos (ejemplo, el disco duro de un servidor, discos dañados que almacenan datos críticos, etc.).

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.
ISO 27001:2022	Apartado 8.1.2 Propiedad de los Activos.

7.11 Servicios de apoyo (Sistema de respaldo eléctrico)

Las instalaciones de procesamiento de la información deberán estar protegidas contra los cortes de energía y otras interrupciones causadas por fallos en los servicios públicos de suministro eléctrico.

Propósito

Prevenir la pérdida, el daño o la puesta en peligro de la información y otros activos asociados, o la interrupción de las operaciones de la institución debido al fallo y la interrupción de los servicios de apoyo.

Orientación

Asegurar que el equipo que soporta los servicios públicos está configurado, operado y mantenido de acuerdo con las especificaciones del fabricante correspondiente.

Garantizar que los servicios públicos sean evaluados periódicamente en cuanto a su capacidad para satisfacer el crecimiento de la empresa y las interacciones con otros servicios de apoyo.

Asegurar que el equipo de apoyo a los servicios públicos sea inspeccionado y probado regularmente para asegurar su correcto funcionamiento; si es necesario, activar las alarmas para detectar el mal funcionamiento de los servicios.

Garantizar que los equipos que soportan los servicios públicos están en una red separada de las instalaciones de procesamiento de la información, si están conectadas a una red.

a) Garantizar que los equipos que soportan los servicios públicos se conecten a Internet sólo cuando sea necesario y de forma segura.
b) Se debe proporcionar iluminación y comunicaciones de emergencia. Los interruptores y válvulas de emergencia para cortar la electricidad, el agua, el gas u otros servicios deben estar situados cerca de las salidas de emergencia o de las salas de equipos.
c) Los detalles de los contactos de emergencia deben estar registrados y disponibles para el personal en caso de que se produzca un apagón.
d) Los equipos deben estar protegidos contra fallos de energía u otras anomalías eléctricas mediante un sistema complementario. Por un lado, existen una serie de generadores eléctricos que entrarían en funcionamiento en caso de fallo en el suministro de energía, por otro lado, existe un sistema de alimentación ininterrumpida (SAI) que permiten la continuidad de los sistemas hasta que entren en funcionamiento los generadores.
e) Se debe garantizar el suministro de agua, necesaria para el funcionamiento de las infraestructuras de climatización.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.
ISO 27001:2022	Apartado 8.1.2 Propiedad de los Activos.

7.12 Seguridad del cableado

El cableado de comunicaciones y energía que transportan datos, energía o servicios de información de apoyo, deben estar protegidos contra la interceptación, las interferencias o los daños.

Propósito

Prevenir la pérdida, el daño, el robo o el compromiso de la información y otros activos asociados, así como la interrupción de las operaciones de la institución relacionadas con el cableado de energía y comunicaciones.

Orientación

Deben tenerse en cuenta las mejores prácticas para la seguridad del cableado.

El ICE posee varias normativas al respecto como son; la “Política de Seguridad de Redes de Comunicaciones” y la “Política Corporativa Sistema de Cableado Estructurado en Edificios”.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.
87.00.001.2023	Política de Seguridad de Redes de Comunicaciones.
24.00.098.2005	Política Corporativa Sistema de Cableado Estructurado en Edificios.
GU-GTSD-SC-SI-001	Guia Mejores Prácticas Ciberseguridad Redes TI
GU-GTSD-SC-SI-003	Guia Mejores Prácticas Ciberseguridad Redes TO

7.13 Mantenimiento del equipo

El equipo debe mantenerse correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información.

Propósito

Prevenir la pérdida, el daño, el robo o el compromiso de la información y otros activos asociados, así como la interrupción de las operaciones de la institución causada por la falta de mantenimiento.

Orientación

El equipo debe mantenerse correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información.

Deben tenerse en cuenta los siguientes controles para el mantenimiento del equipo:

a) Para asegurar una continua disponibilidad e integridad de la información, el ICE realiza un mantenimiento preventivo y correctivo de sus equipos. Estos mantenimientos son realizados directamente por cada una de las dependencias técnicas del ICE, siguiendo las pautas establecidas por la Dirección de Soluciones Tecnológicas de la Gerencia Tecnología y Soluciones Digitales, y en los casos que corresponda, intervienen terceros con los que existe una relación contractual, además, hay casos en los que los servicios son prestados por otra dependencia de la institución.

b) En los contratos con terceros se debe hacer mención expresa al deber de confidencialidad con respecto a la información a la que tenga acceso para el cumplimiento de las obligaciones contractuales.

Mantenimiento Correctivo

a) De los mantenimientos correctivos queda evidencia documental, bien en los registros de mantenimiento proporcionados por la empresa proveedora o socio comercial que los realiza o mediante el registro en protocolos propios del ICE. Dependerá de quién haya solucionado dicha incidencia.

b) El mantenimiento correctivo tanto en hardware como en software es responsabilidad de la Dirección de Soluciones Tecnológicas de la Gerencia Tecnología y Soluciones Digitales.

Mantenimiento Preventivo

Las tareas de mantenimiento preventivo están establecidas en función de:

a) Las operaciones recomendadas por el fabricante o suministrador.

b) El análisis de los fallos ocurridos: número de fallos, número de paradas, costes de reparación, etc.

c) La programación de las intervenciones o cambios se hace de forma coordinada, a fin de utilizar los tiempos o épocas de no uso o las que éste es menor. Estas intervenciones están detalladas en los contratos y acuerdos de mantenimiento suscritos con las empresas contratadas a tal efecto.

Cuando realizada la intervención de mantenimiento preventivo, se detecten fallos o elementos que deban sustituirse, se programarán dichas acciones con el titular subordinado del proceso afectado, de tal manera que la continuidad de negocio se vea afectada lo menos posible. El Coordinador del cambio es quien se encarga de que se realicen las correspondientes pruebas antes de la puesta en servicio.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.
ISO 27001:2022	Apartado 8.1.2 Propiedad de los Activos.

7.14 Eliminación segura o reutilización del equipo

Los equipos que contengan medios de almacenamiento deben ser verificados para garantizar que cualquier información sensible y software con licencia haya sido eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.

Propósito

Para evitar la fuga de información de los equipos que van a ser eliminados o reutilizados.

Orientación

El equipo debe ser verificado para asegurar la contención de los medios de almacenamiento antes de su eliminación o reutilización. Los soportes de almacenamiento que contengan información confidencial o protegida por derechos de autor deben ser destruidos físicamente o la información debe ser destruida, borrada o sobrescrita

utilizando técnicas para que la información original no sea recuperable en lugar de utilizar la función de borrado estándar.

El ICE debe considerar la eliminación tanto de los controles de seguridad, como los controles de acceso y/o los equipos de vigilancia, al final del contrato de arrendamiento o cuando se traslade de locales. Esto depende de factores como:

a) Su contrato de arrendamiento para devolver las instalaciones a su estado original.
b) Minimizar el riesgo de dejar los sistemas con información sensible para el siguiente inquilino (por ejemplo, listas de acceso de usuarios, archivos de vídeo o imágenes).
c) La posibilidad de reutilizar los controles en la siguiente instalación.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.
ISO 27001:2022	Apartado 8.1.2 Propiedad de los Activos.

8 CONTROLES TECNOLÓGICOS

8.1 Dispositivos de punto final del usuario

La información almacenada, procesada o accesible a través de los dispositivos de los usuarios debe estar protegida.

Propósito

Para proteger la información contra los riesgos introducidos por el uso de dispositivos de punto final del usuario.

Orientación

ICE debe establecer una normativa específica sobre la configuración y el manejo seguro de los dispositivos de punto final de los usuarios.

La normativa específica del tema debe ser comunicada a todo el personal.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.
87.00.001.2022	Reglamento del Uso de Información del ICE mediante Dispositivos Móviles.
ISO 27001:2022	Apartado 8.1.2 Propiedad de los Activos.

8.2 Derechos de acceso privilegiados

La asignación y el uso de los derechos de acceso privilegiados deben ser restringidos y gestionados.

Propósito

Para garantizar que sólo los usuarios autorizados, los componentes de software y los servicios tengan derechos de acceso privilegiados.

Orientación

La asignación de derechos de acceso privilegiados debe controlarse mediante un proceso de autorización de acuerdo con la normativa específica del tema correspondiente sobre el control de acceso.

A continuación, algunos controles a tomar en cuenta:

a) Identificar aquellas cuentas administrativas locales que nunca deben ser utilizadas para el trabajo diario y, solo deben estar ahí para aquellos momentos puntuales y documentados en los que sea necesario llevar a cabo labores de administración.

b) Identificar las cuentas de usuario con privilegios ya que son el objetivo más común de ataques de phishing dirigidos, dado que la mayoría de éstos están asignados a usuarios que no son profesionales de Tecnologías, ni tienen formación específica en ciberseguridad.

c) Identificar las cuentas administrativas de dominio, es una cuenta de administración con privilegios en todos los componentes del dominio y es cuenta no personal, que no debe ser de uso constante y que actúa a modo de llave maestra para el administrador de esa infraestructura.

d) Identificar las cuentas servicio externo, en especial aquellos en la nube (modelo “as service”), donde cada vez más elementos de las infraestructuras tecnológicas dependen de proveedores externos. Muchas veces esos servicios externos almacenan y gestionan activos importantes y que deben estar bien protegidos.

e) Identificar las cuentas de usuarios con privilegios temporales y de emergencia que son asignados en respuesta a una incidencia, por una necesidad puntual, deben recibir la supervisión adecuada durante su habilitación. Además, es necesario una gestión adecuada, para evitar mantener los privilegios durante más tiempo del que los necesitan.

f) Identificar las cuentas de aplicación/servicio, es decir aquellas que no son operados por personas, sino por software, por ejemplo, las claves SSH o API keys que se emplean para interconectar elementos de iCloud con otros de nuestra propia infraestructura.

g) Restringir y controlar la asignación y uso de los derechos de acceso privilegiados.

h) Definir los requisitos para la expiración de los derechos de acceso privilegiados.

i) Revisar constantemente las cuentas de los usuarios con los accesos privilegiados activas y determinar si están alineadas a las funciones y roles para las que fueron establecidas.

j) Establecer las responsabilidades ante el uso de los accesos privilegiados y las posibles sanciones e implicaciones legales respectivas en caso de comprobarse un uso inadecuado o no autorizado.

k) Revisar y garantizar que cada cuenta de usuario tiene los privilegios de accesos debidamente autorizados para desempeñar las labores propias al cargo para el cual fue contratado.

l) Ejecutar inmediatamente el retiro o bloqueo de los accesos de las cuentas de usuario que han cambiado de funciones, o que se retiran de la institución.

m) Se debe mantener el escritorio del computador, sin documentos, carpetas y/o accesos directos a información clasificada o reservada.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.
87.00.001.2022	Reglamento del Uso de Información del ICE mediante Dispositivos Móviles.

8.3 Restricción del acceso a la información

El acceso a la información y a otros activos asociados debe estar restringido de acuerdo con la normativa específica establecida sobre el control de acceso.

Propósito

Garantizar la seguridad e integridad de los datos institucionales y los activos de información del ICE. Todos los recursos tecnológicos del ICE se adherirán a un estándar y marco de control de acceso uniforme.

Orientación

Este control del ICE procura que toda la información, independientemente del formato (electrónico, papel, etc.) se creará, recopilará, mantendrá y administrará de manera segura, según los siguientes controles:

a) Todos los dispositivos y aplicaciones de software que se conecten a la red del ICE deberán proporcionar autenticación de usuario y control de acceso únicamente a través de los Procedimientos de Control de Acceso del ICE aprobados. La

validación de los protocolos de gestión de identidad reside en el Proceso Seguridad Informática.

b) Las excepciones a este control y los procedimientos asociados solo se permitirán si el Proceso Seguridad Informática las aprueba previamente y el director de Ciberseguridad documente y verifique esta aprobación.

c) Los funcionarios que infrinjan este control del ICE pueden estar sujetos a medidas disciplinarias por mala conducta y/o desempeño en función del proceso administrativo correspondiente a su trabajo.

d) Los funcionarios y trabajadores también pueden estar sujetos a la interrupción de los servicios de tecnología de la información específicos en función de la violación de este control.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.
87.00.001.2022	Reglamento del Uso de Información del ICE mediante Dispositivos Móviles.

8.4 Acceso al código fuente

El acceso de lectura y escritura al código fuente, a las herramientas de desarrollo y a las bibliotecas de software debe gestionarse adecuadamente.

Propósito

Controlar el acceso al código fuente y elementos asociados para evitar la introducción de funciones no autorizadas, evitar cambios no intencionales o maliciosos y mantener la confidencialidad de la propiedad intelectual valiosa.

Orientación

El acceso al código fuente y elementos asociados (como diseños, especificaciones, planes de verificación y planes de validación) y herramientas de desarrollo (por ejemplo, compiladores, constructores, herramientas de integración, plataformas y entornos de prueba) debe controlarse estrictamente.

Para el correcto aseguramiento del código fuente, es necesario asegurar y controlar el almacenamiento central de dicho código, preferiblemente desde el mismo sistema de gestión de código fuente. Para ello, se deberá realizar lo siguiente:

a) Se deben especificar permisos de acceso para usuarios con un rol determinado en el nivel del repositorio o en el nivel de ruta dentro de un repositorio donde se encuentre el código fuente.

b) Cuando se establece un permiso para un rol en cualquier directorio del repositorio, todos los directorios y archivos de ese directorio obtienen el mismo permiso.

c) Cuando se establece un permiso en un archivo individual en el repositorio, no hay efecto en los permisos asignados a las rutas por encima del nivel de ese archivo.

d) La forma en que utilicen los permisos basados en rutas dependerá de si ve los permisos principalmente como una forma de otorgar acceso o como una forma de restringir el acceso.

   a. Acceso completo, con excepciones

      Proporcionar a los funcionarios y trabajadores de la institución acceso a la base de código fuente completa, al tiempo que permite a los desarrolladores de las empresas contratistas comprometerse solo con aquellas partes de la base de código en las que se espera que trabajen.

   b. Sin acceso, con excepciones

      Asigne a todos los desarrolladores "Sin acceso" de forma predeterminada, luego asigne cada tipo de acceso de desarrollador a ciertos directorios y archivos de acuerdo con sus responsabilidades.

   c. Cuando niega todo acceso a un repositorio para un rol, los usuarios con ese rol no pueden ver que el repositorio existe, excepto si:

      El rol tiene acceso de "ver y confirmar" a algún directorio dentro del repositorio. En este caso, los usuarios con este rol pueden ver los directorios que contienen el directorio al que tienen acceso.

   a. El usuario tiene otro rol que otorga acceso a alguna parte del repositorio.

      Los usuarios con un rol que tiene acceso de "solo lectura" a una ruta pueden explorar el contenido del repositorio en el sitio web o conectándose directamente al repositorio desde un cliente.

d. Los usuarios con un rol que tiene el permiso "ver y confirmar" en una ruta pueden buscar y descargar código, y también pueden verificar el código en el repositorio.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

8.5 Autenticación segura

Las tecnologías y los procedimientos de autenticación segura deben aplicarse en función de las restricciones de acceso a la información y de la normativa específica de control de acceso.

Propósito

El propósito de este control de autenticación segura es garantizar la integridad de los datos y los recursos de tecnología de la información en el ICE al garantizar los controles para proteger las credenciales de identificación y autenticación del usuario. El ICE utilizará los tres métodos básicos de autenticación: algo que la persona sabe (es decir, una contraseña), algo que la persona tiene (es decir, una tarjeta inteligente o identificación) y algo que la persona es (es decir, una huella dactilar u otros datos biométricos). Para garantizar la seguridad y la integridad de los datos, los usuarios identificados se autenticarán de forma segura en los recursos de tecnología de la información y accederán solo a los recursos a los que han sido autorizados a acceder. Este control mitigará el riesgo de acceso no autorizado a la información, así como también establecerá la responsabilidad del usuario y las reglas de acceso.

Orientación

A continuación, algunas pautas:

a) El ICE exigirá que los sistemas estén protegidos contra el acceso no autorizado mediante el establecimiento de requisitos para la autorización y gestión de cuentas de usuario, proporcionando autenticación de usuario (cualquiera o todos los métodos básicos de autenticación) e implementando controles de acceso a los

recursos de tecnología de la información de ICE. El control de acceso se proporciona en los niveles de firewall, red, sistema operativo y aplicación.

b) Los titulares subordinados del ICE tienen la responsabilidad de solicitar acceso a los sistemas de información y aprobar los privilegios de acceso de los usuarios en función de sus deberes asignados, así como notificar a los responsables de la información y a TI sobre la finalización del acceso a los recursos de tecnología de la información.

c) Antes de que se les otorgue acceso a los recursos de tecnología de la información, las necesidades del funcionario, trabajador, proveedor, socio comercial, invitado o voluntario se considerarán ampliamente y se otorgará la autorización para permitir el acceso a los recursos de tecnología de la información. El acceso debe otorgarse de acuerdo con el principio del mínimo privilegio.

d) Las cuentas del ICE tendrán un identificador único asociado con un solo usuario. Una vez que se asigna un identificador a una persona en particular, siempre se asocia con esa persona. Nunca se reasigna posteriormente para identificar a otra persona.

e) El uso del servicio de autenticación ante un sistema en el ICE constituye una identificación oficial del usuario ante la institución, de la misma forma que lo hace la presentación de una cédula de identidad. La seguridad es responsabilidad de todos, y todos tienen la responsabilidad de proteger su propia “identidad”. Los usuarios serán responsables de todas las acciones de sus cuentas.

f) Independientemente del método de autenticación utilizado, los usuarios deben usar solo la información de autenticación para la que han sido autorizados; es decir, nunca debe identificarse falsamente como otra persona. Además, los usuarios deben mantener la confidencialidad de su información de autenticación; es decir, no debe ponerlo a disposición de una persona no autorizada a sabiendas o por negligencia. Cualquier persona que sospeche que su información de autenticación se ha visto comprometida debe comunicarse con el CSIRT de inmediato.

g) Los usuarios deben cumplir con los requisitos del control de contraseñas seguras.

h) Los responsables de información empresarial deben garantizar que los procesos de autorización y gestión de cuentas estén documentados y que se haya asignado a las personas adecuadas la responsabilidad de crear y mantener registros de autorización.

i) Los responsables de información empresarial pueden monitorear las actividades relacionadas de las personas como condición para el acceso continuo. Los

responsables de información del ICE deberán revisar los privilegios de acceso de los usuarios como mínimo una vez al año.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

8.6 Gestión de la capacidad

El uso de los recursos debe ser supervisado y ajustado en función de las necesidades de capacidad actuales y previstas.

Propósito

Este control establece el deber de la institución para planificar y ejecutar el proceso de gestión de la capacidad para garantizar que todos los aspectos actuales y futuros de ésta, y el rendimiento de la infraestructura tecnológica se proporcionen para cumplir con los objetivos de negocio a un costo aceptable. El proceso de gestión de la capacidad garantiza que la infraestructura tecnológica se proporcione en el momento adecuado en el volumen correcto al precio correcto y garantiza que las tecnologías se utilicen de la manera más eficiente.

Orientación

a) Toda organización de TI que tenga la responsabilidad de la capacidad de TI debe seguir los procesos de ésta.

b) Los negocios tienen la responsabilidad de obtener financiamiento para respaldar sus necesidades de infraestructura de capacidad de TI. Esto incluye la adquisición inicial, así como las necesidades de mantenimiento.

c) El desarrollo de requisitos de TI será preciso al implementar la forma más rentable de respaldar las necesidades de capacidad de TI de los negocios.

d) La adquisición de capacidad de TI en apoyo del negocio será de acuerdo con los estándares de la industria y al mejor costo posible.

e) Mantener la capacidad de TI en línea con los acuerdos de nivel de servicio entre el negocio y el soporte de capacidad de TI.

f) Modernizar la capacidad de TI para respaldar el negocio de la manera más eficiente y rentable.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

8.7 Protección contra el programa maligno

La protección contra los programas maliciosos debe ser implementada y apoyada por una adecuada concientización de los usuarios.

Propósito

Este control proporciona detalles de cómo debe regir la operación y el uso de software diseñado específicamente para proteger los sistemas de información del ICE de software malicioso.

Orientación

La protección contra el programa maligno debe basarse en el software de detección y reparación de programa maligno, la concientización sobre la seguridad de la información, el acceso adecuado al sistema y los controles de gestión de cambios. El uso de software de detección y reparación de programa maligno por sí solo no suele ser adecuado. Se debe tener en cuenta la siguiente orientación:

a) El software antivirus institucional debe instalarse y configurarse correctamente en todos los puntos finales y servidores admitidos en la red ICE de acuerdo con los requerimientos de fábrica de cada elemento.

b) El software antivirus debe mantenerse actualizado.

c) Las actualizaciones de software antivirus deben implementarse en la red automáticamente después de recibirlas del proveedor y debe configurarse para verificar estas actualizaciones cada 24 horas.

d) El software antivirus debe configurarse para escaneos en tiempo real y escaneos regulares programados.

e) El escaneo on-access debe configurarse dentro del software antivirus para medios extraíbles y sitios web. El servidor antivirus debe ser monitoreado diariamente por un administrador de TI para detectar alertas de virus. En caso de infección por un virus que infecte varios dispositivos (más de 3 dispositivos) al mismo tiempo. El oficial de protección de datos debe completar un informe de análisis de causa raíz.

f) La protección contra manipulaciones debe estar habilitada para evitar que los usuarios finales o el programa maligno alteren la configuración del software antivirus o deshabiliten la protección.

g) Todos los equipos de TI y los medios extraíbles deben escanearse en busca de virus y programa maligno antes de introducirlos o usarlos en la red por primera vez.

h) Los usuarios no deben aceptar ni ejecutar software de fuentes que no sean de confianza.

i) Los usuarios no deben realizar ninguna actividad con la intención de crear y/o distribuir programas maliciosos (por ejemplo, virus, gusanos, troyanos, bombas de correo electrónico, etc.) en las redes o sistemas.

j) Los usuarios deben informar a seguridad informática inmediatamente si se detecta un virus en su sistema.

k) Los sistemas de TI infectados con programa maligno/virus que no haya sido detectado por el software antivirus deben desconectarse/ponerse en cuarentena de la red de la institución hasta que estén libres de virus.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
SC.CDSE.021.2019	Lineamientos para la Atención de Incidentes de Seguridad de la Información y Ciberseguridad.

Código	Ley, Política, Norma
SC.CDSE.009.2019	Proceso de Manejo de Incidentes de Seguridad de la Información.
SC.CDSE.010.2019	Procedimiento Valoración y Ajuste a la Infraestructura.
SC.CDSE.011.2019	Procedimiento Detección y Análisis de Incidentes.
SC.CDSE.012.2019	Procedimiento Contención.
SC.CDSE.013.2019	Procedimiento Investigación de Incidentes de Seguridad de la Información.
SC.CDSE.014.2019	Procedimiento Erradicación de Incidentes de Seguridad.
SC.CDSE.015.2019	Procedimiento Recuperación de Incidentes de Seguridad de la Información.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.
87.00.001.2022	Reglamento del Uso de Información del ICE mediante Dispositivos Móviles.

8.8 Gestión de las vulnerabilidades técnicas

Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, evaluar la exposición de la institución a dichas vulnerabilidades y tomar las medidas adecuadas.

Propósito

La gestión de vulnerabilidades es la actividad de remediar/controlar las vulnerabilidades de seguridad, entre otros, de la siguiente manera:

a) Identificar la exploración de redes, sistemas y aplicaciones en busca de vulnerabilidades conocidas.

b) Identificar oportunamente las vulnerabilidades del sistema es clave para la protección y seguridad de los recursos de la institución para el acceso continuo a ellos.

Orientación

Toda la infraestructura de red, los servidores, los sistemas operativos en máquinas virtuales, los sistemas operativos de servidores alojados en la nube, los servidores de

bases de datos, las bases de datos y las aplicaciones del ICE deben monitorearse de manera continua.

Los sistemas con datos de alto riesgo deben escanearse en busca de vulnerabilidades al menos una vez al mes.

El CSIRT del ICE realiza escaneos regulares autenticados y no autenticados de redes, sistemas, bases de datos o aplicaciones. Las dependencias que administran redes, sistemas, bases de datos o aplicaciones deben usar el servicio de escaneo del CSIRT o realizar escaneos similares. Los escaneos se limitan a revisar la configuración del sistema y la aplicación y no abren ni examinan el contenido de correos electrónicos, documentos, hojas de cálculo, bases de datos o cualquier otra aplicación.

Las vulnerabilidades de seguridad identificadas a través de escaneos o identificadas por proveedores, se deben comunicar vía informe para remediar o controlar como se describe a continuación.

a) Escaneos de Vulnerabilidad
    a. Exploraciones de vulnerabilidad de red no autenticadas.
    b. Escaneo de vulnerabilidades de red autenticadas.
    c. Escaneo de seguridad de aplicaciones web.
    d. Escaneos dirigidos para vulnerabilidades específicas
b) Remediación de vulnerabilidades y mitigación de riesgos:
    a. Si un análisis de vulnerabilidades identifica amenazas en un área o dependencia del ICE o éstas se enteran de nuevas vulnerabilidades, se espera que la dependencia/persona de TI responsable las solucione o, en los casos excepcionales en los que eso no sea posible, implemente controles compensatorios aprobados y documentados para reducir el riesgo. En los casos en que una vulnerabilidad presente un mayor riesgo para la exposición de los datos, seguridad informática puede desconectar, deshabilitar y/o bloquear el acceso del dispositivo a seguridad informática hasta que se lleve a cabo la reparación o la mitigación del riesgo.
    b. Priorizar según la gravedad: Se alienta a los destinatarios del informe de análisis de vulnerabilidades a priorizar los esfuerzos de remediación en función de la gravedad de la vulnerabilidad y el impacto potencial en la confidencialidad, integridad o disponibilidad de los sistemas vulnerables y/o sus datos. La gravedad de la vulnerabilidad está determinada por la calificación proporcionada por el Sistema de Puntuación de Vulnerabilidad Común (CVSS) del Instituto Nacional de Estándares y Tecnología (NIST). Se debe dar la máxima prioridad a las vulnerabilidades calificadas como Críticas (CVSS 9-10) o Altas (CVSS 7-8.9).

c. Plan de remediación/mitigación de riesgos: la planificación de la remediación debe:
   - Validar que la vulnerabilidad esté debidamente identificada y priorizada.
   - Incluir las acciones específicas que se tomarán para mitigar el riesgo que plantea la vulnerabilidad.
   - Asegurar que los recursos apropiados estén o estarán, disponibles para remediar la vulnerabilidad o mitigar el riesgo que plantea la vulnerabilidad.
   - Identificar hitos en el proceso de remediación/mitigación de riesgos para abordar completamente la vulnerabilidad.

d. Asegurar que el cronograma para resolver o abordar la vulnerabilidad sea alcanzable y permita las pruebas adecuadas.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
SC.CDSE.021.2019	Lineamientos para la Atención de Incidentes de Seguridad de la Información y Ciberseguridad.
SC.CDSE.009.2019	Proceso de Manejo de Incidentes de Seguridad de la Información.
SC.CDSE.010.2019	Procedimiento Valoración y Ajuste a la Infraestructura.
SC.CDSE.011.2019	Procedimiento Detección y Análisis de Incidentes.
SC.CDSE.012.2019	Procedimiento Contención.
SC.CDSE.013.2019	Procedimiento Investigación de Incidentes de Seguridad de la Información.
SC.CDSE.014.2019	Procedimiento Erradicación de Incidentes de Seguridad.
SC.CDSE.015.2019	Procedimiento Recuperación de Incidentes de Seguridad de la Información.

Código	Ley, Política, Norma
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.
87.00.001.2022	Reglamento del Uso de Información del ICE mediante Dispositivos Móviles.

8.9 Gestión de la configuración

Las configuraciones, incluidas las de seguridad, del hardware, el software, los servicios y las redes deben establecerse, documentarse, aplicarse, supervisarse y revisarse.

Propósito

El propósito de este control es establecer los requisitos obligatorios para la instalación, configuración e implementación de sistemas de tecnología de la información en el ICE.

Orientación

La gestión de la configuración se centra en establecer y mantener la coherencia entre los atributos funcionales de un sistema y sus requisitos a lo largo de su ciclo de vida. Este control establece la guía para que en el ICE se garantice que las configuraciones se controlen adecuadamente y se mantengan con precisión para la prestación exitosa de los servicios.

a) Los procesos de configuración deben incorporar las mejores prácticas aplicables de la industria, que respaldan la disponibilidad óptima del sistema de producción y la gestión eficaz del sistema. Estas prácticas incluyen:
    - Usar métodos, procesos y procedimientos estandarizados y documentados.
    - Rastrear y comunicar de manera efectiva todos los cambios del sistema realizados en hardware, software, firmware y documentación, a través de la planificación, aprobación, notificación, desarrollo, prueba, programación y gestión de la implementación de cambios.
    - Tomar decisiones efectivas basadas en el riesgo para mantener la capacidad de misión de cada sistema, la postura de seguridad autorizada y el riesgo minimizado.
    - Maximizar los recursos del ICE.
b) Se debe utilizar una base de datos de gestión de la configuración (CMDB) que contenga y realice un seguimiento de la información relevante sobre los elementos

de configuración, sus atributos, las líneas base, la documentación, los cambios y las relaciones. Los sistemas existentes o nuevos pueden cumplir este requisito.

c) La adhesión a esta base de datos garantiza que los siguientes aspectos se aborden adecuadamente:
   - Líneas base de configuración del sistema
   - Supervisión de la configuración
   - Requisitos de comunicación
     - Conectividad de red
     - Ubicación
     - Equipo
     - Requisitos de la aplicación / sistema operativo
   - Seguridad
     - Autenticación
     - Cifrado
     - Publicaciones/Servicios/Protocolos
   - Aplicaciones
     - Instalación
     - Configuración
     - Seguridad

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
SC.CDSE.021.2019	Lineamientos para la Atención de Incidentes de Seguridad de la Información y Ciberseguridad.
SC.CDSE.009.2019	Proceso de Manejo de Incidentes de Seguridad de la Información.

Código	Ley, Política, Norma
SC.CDSE.010.2019	Procedimiento Valoración y Ajuste a la Infraestructura.
SC.CDSE.011.2019	Procedimiento Detección y Análisis de Incidentes.
SC.CDSE.012.2019	Procedimiento Contención.
SC.CDSE.013.2019	Procedimiento Investigación de Incidentes de Seguridad de la Información.
SC.CDSE.014.2019	Procedimiento Erradicación de Incidentes de Seguridad.
SC.CDSE.015.2019	Procedimiento Recuperación de Incidentes de Seguridad de la Información
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.
87.00.001.2022	Reglamento del Uso de Información del ICE mediante Dispositivos Móviles.

8.10 Eliminación de información

La información almacenada en los sistemas de información, en los dispositivos o en cualquier otro medio de almacenamiento debe ser eliminada cuando ya no sea necesaria.

Propósito

El objetivo del presente documento es garantizar que la información almacenada en equipos y soportes sea borrada o eliminada de forma segura.

Orientación

a) Todos los datos y software con licencia almacenado en soportes móviles (por ej., CD, DVD, unidades USB, tarjetas de memoria, etc., y también en papel) y en todos los equipos que tienen soportes de almacenamiento de información (por ejemplo, computadoras, teléfonos móviles, etc.) deben ser borrados, o se debe destruir el respaldo, antes de ser eliminados o reutilizados.

b) Se debe definir el responsable de verificar y borrar datos de los diferentes sistemas del ICE.

c) La persona responsable de borrar los datos o destruir el soporte debe informar al propietario del activo en cuestión acerca del borrado o eliminación de datos, y el propietario del activo debe actualizar el Inventario de activos.

d) Se debe definir para cada sistema de información la tecnología utilizada para el borrado de información.

e) Los datos deben ser borrados, teniendo en cuenta su sensibilidad.

f) Los funcionarios o trabajadores de la institución que manejan documentos individuales son responsables de destruir los soportes en papel, salvo que la normativa de clasificación de la información establezca otra cosa. La información en papel se destruye en trituradoras de papel.

g) Se deben llevar registros de todo el borrado o destrucción de datos clasificados como "Privado" y "Confidencial". Los registros deben incluir la siguiente información:

- datos sobre los soportes, fecha de borrado o destrucción.
- método de borrado o destrucción.
- persona que realizó el proceso.

h) Toda la información clasificada como "Confidencial" debe ser borrada o destruida ante la presencia de una comisión integrada por personas autorizadas a acceder a dicha información.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
SC.CDSE.021.2019	Lineamientos para la Atención de Incidentes de Seguridad de la Información y Ciberseguridad.
SC.CDSE.009.2019	Proceso de Manejo de Incidentes de Seguridad de la Información.
SC.CDSE.010.2019	Procedimiento Valoración y Ajuste a la Infraestructura.
SC.CDSE.011.2019	Procedimiento Detección y Análisis de Incidentes.
SC.CDSE.012.2019	Procedimiento Contención.
SC.CDSE.013.2019	Procedimiento Investigación de Incidentes de Seguridad de la Información.

Código	Ley, Política, Norma
SC.CDSE.014.2019	Procedimiento Erradicación de Incidentes de Seguridad.
SC.CDSE.015.2019	Procedimiento Recuperación de Incidentes de Seguridad de la Información.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.
87.00.001.2022	Reglamento del Uso de Información del ICE mediante Dispositivos Móviles.

8.11 Enmascaramiento de datos

El enmascaramiento de datos debe utilizarse de acuerdo con las buenas prácticas normalmente aceptadas y otras normativas específicas del tema, así como con los requisitos de negocio, teniendo en cuenta la legislación aplicable.

Propósito

El objetivo de este control es definir como la institución realiza el enmascaramiento de datos para ocultar los datos según su clasificación, para agregar esta práctica a la estrategia de seguridad de la información institucional cuya función principal es proteger la información confidencial y privada en situaciones en las que podría ser visible para alguien sin autorización para la información.

Orientación

El ICE debe de adoptar las siguientes mejores prácticas para crear una estrategia que funcione para el enmascaramiento de bases de datos dentro de la institución:

a) De primera mano se debe de definir los tipos de data masking (estático o dinámico).
b) Definir las técnicas para enmascarar datos según lo que sea necesario para la institución:
    - Encriptación
    - Scramble de personajes
    - Anulación o eliminación
    - Varianza
    - Sustitución
    - Shuffling

c) Buscar datos; este primer paso consiste en identificar y catalogar los diversos tipos de datos que pueden ser confidenciales. Esto a menudo lo llevan a cabo analistas de seguridad que elaboran una lista completa de elementos de datos de toda la empresa.

d) Evaluar la situación; se requiere la supervisión del administrador de seguridad que es responsable de determinar si hay información confidencial, la ubicación de los datos y la técnica ideal de enmascaramiento de datos.

e) La implementación debe tener en cuenta la arquitectura, la planificación adecuada y una mirada a las necesidades futuras de la empresa.

f) Probar los resultados de enmascaramiento de datos, es el paso final en el proceso. El control de calidad y las pruebas son necesarias para garantizar que las configuraciones de enmascaramiento produzcan los resultados deseados.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
Ley 8968	Ley Protección de las Personas frente al Tratamiento de los Datos Personales.
GDPR	Regulación de Protección de Datos Generales de la Unión Europea.
(NIST) 800-53	Control de Privacidad y Seguridad para Sistemas de Organización Federal y Organizaciones.

8.12 Prevención de la fuga de datos

Las medidas de prevención de fugas de datos deben aplicarse a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información importante para la institución.

Propósito

Detectar e impedir la divulgación y extracción no autorizada de información por parte de individuos o sistemas.

Orientación

La institución debe considerar lo siguiente para reducir el riesgo de fuga de datos:

a) Identificar y clasificar la información para protegerla contra las fugas (por ejemplo, información personal, modelos de precios y diseños de productos).

b) Controlar los canales de fuga de datos (por ejemplo, el correo electrónico, las transferencias de archivos, los dispositivos móviles y los dispositivos de almacenamiento portátiles).

c) Actuar para evitar que se filtre la información (por ejemplo, poner en cuarentena los correos electrónicos que contengan información sensible).

Las herramientas de prevención de fugas de datos deben utilizarse para:

a) Identificar y controlar la información sensible que corre el riesgo de ser revelada sin autorización (por ejemplo, en los datos no estructurados del sistema de un usuario).

b) Detectar la divulgación de información sensible (por ejemplo, cuando la información se sube a servicios en la nube de terceros que no son de confianza o se envía por correo electrónico).

c) Bloquear las acciones de los usuarios o las transmisiones de la red que expongan información sensible (por ejemplo, impedir que se copien las entradas de la base de datos en una hoja de cálculo).

La institución debe determinar si es necesario restringir la capacidad de un usuario para copiar y pegar o cargar datos en servicios, dispositivos y medios de almacenamiento fuera de la institución. Si ese es el caso, la institución debe implementar tecnología como herramientas de prevención de fuga de datos o la configuración de las herramientas existentes que permitan a los usuarios ver y manipular los datos mantenidos de forma remota pero que impidan copiar y pegar fuera del control de la institución.

Si la exportación de datos es necesaria, el propietario de los datos debe poder aprobar la exportación y hacer que los usuarios sean responsables de sus acciones.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

Código	Ley, Política, Norma
Ley 8968	Ley Protección de las Personas frente al Tratamiento de los Datos Personales.
GDPR	Regulación de Protección de Datos Generales de la Unión Europea.
(NIST) 800-53	Control de Privacidad y Seguridad para Sistemas de Organización Federal y Organizaciones.
19.00.001.2017	Lineamientos para el Funcionamiento del Modelo de Arquitectura de Información Empresarial para el Grupo ICE.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.

8.13 Respaldo de información

Las copias de seguridad de la información, los programas informáticos y los sistemas deben mantenerse y probarse periódicamente de acuerdo con la normativa específica acordada sobre las copias de seguridad.

Propósito

El propósito de este control es estandarizar los procedimientos de respaldo, prueba y recuperación de datos, que protegen los sistemas de información, redes, datos, bases de datos y otros activos de información del ICE.

La normativa adicional que rige las actividades específicas de recuperación ante desastres (DR) se abordarán por separado.

Orientación

Los custodios de la información son los responsables de proporcionar respaldos de seguridad adecuadas para garantizar la recuperación de la información electrónica en caso de falla. Estas disposiciones de respaldo permitirán que los procesos críticos del ICE se reanuden en un período de tiempo razonable con una pérdida mínima de datos. Dado que las fallas pueden tomar muchas formas y pueden ocurrir con el tiempo, se deben mantener múltiples instancias de respaldos de seguridad.

a) La institución desarrollará planes completos de respaldos de seguridad de datos de acuerdo con las buenas prácticas de gestión de respaldos de seguridad y recuperación de datos definidas en las buenas prácticas.

b) Las actividades de copia de seguridad y recuperación de datos se realizarán como parte de la gestión de continuidad del negocio y los planes de recuperación ante desastres (DRP) del ICE, que administran y gestionan el programa general de copia de seguridad de datos de tecnología, que incluye:
   - Planificación y diseño de actividades de respaldo y recuperación de datos.
   - Identificación de equipos de respaldo de datos, definiendo sus roles y responsabilidades y asegurando que estén debidamente capacitados y preparados para responder a un incidente.
   - Planificación, diseño y documentación de planes de respaldo y recuperación de datos.
   - Programación de actualizaciones de los análisis de impacto al negocio de copia de seguridad y recuperación de datos.
   - Programación de actualizaciones de las evaluaciones de riesgos de respaldo y recuperación de datos.
   - Planificación y entrega de actividades de concientización y capacitación para funcionarios y miembros del equipo de respaldo de datos.
   - Planificación y diseño de actividades de respuesta a incidentes asociadas con la copia de seguridad y recuperación de datos.
   - Planificación y ejecución de ejercicios de plan de respaldo y recuperación de datos.
   - Diseñar e implementar un programa de respaldo y recuperación de datos/actividad de mantenimiento del plan para garantizar que los planes estén actualizados y listos para usar.
   - Preparación para la revisión por parte del titular subordinado y la auditoría de los planes de respaldos de seguridad y recuperación de datos.
   - Planificación e implementación de actividades de mejora continua para el programa y los planes de copia de seguridad y recuperación de datos.

c) Se llevará a cabo una evaluación de riesgos y un análisis de impacto al negocio, formales para determinar los requisitos para todos los planes de respaldos de seguridad y recuperación de datos; los análisis de riesgos y los análisis de impacto al negocio, se actualizarán al menos una vez al año para garantizar que estén alineados con el negocio y sus requisitos tecnológicos.

d) Las estrategias para responder a incidentes tecnológicos específicos, tal como se define en el análisis de riesgos y los análisis de impacto al negocio, se identificarán y utilizarán al desarrollar planes individuales de copia de seguridad y recuperación de datos.

e) Los planes de copia de seguridad y recuperación de datos abordarán la copia de seguridad y la recuperación de elementos tecnológicos críticos, incluidos sistemas, redes, bases de datos y datos, de acuerdo con las actividades comerciales clave.

f) Los planes de respaldos de seguridad y recuperación de datos se probarán periódicamente en un entorno adecuado para garantizar que los sistemas, las redes, las bases de datos y otros elementos de la infraestructura puedan recuperarse y volver a su estado normal en situaciones de emergencia y que los funcionarios del ICE entiendan cómo se van a ejecutar los planes, así como sus funciones y responsabilidades.

g) Todos los funcionarios y trabajadores deben conocer el programa y los planes de copia de seguridad y recuperación de datos y sus propias funciones y responsabilidades durante un incidente.

h) Los planes de respaldo y recuperación de datos y otros documentos deben mantenerse actualizados y reflejarán las circunstancias existentes y cambiantes.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
Ley 8968	Ley Protección de las Personas frente al Tratamiento de los Datos Personales.
GDPR	Regulación de Protección de Datos Generales de la Unión Europea.
(NIST) 800-53	Control de Privacidad y Seguridad para Sistemas de Organización Federal y Organizaciones.
19.00.001.2017	Lineamientos para el Funcionamiento del Modelo de Arquitectura de Información Empresarial para el Grupo ICE.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.

8.14 Redundancia de las instalaciones de procesamiento de información

Las instalaciones de procesamiento de la información deben implementarse con una redundancia suficiente para cumplir con los requisitos de disponibilidad.

Propósito

Es imperativo que se tengan facilidades alternas que brinden redundancia a las instalaciones para asegurar la continua operación de las instalaciones de proceso de información.

Orientación

Este control aplica para las áreas de Data Center del ICE a saber:

a) Identificar los requisitos para la disponibilidad de los servicios de negocio y los sistemas de información.

b) Implementar una arquitectura de sistemas con la redundancia adecuada para cumplir con estos requisitos.

c) Establecer una relación comercial con dos proveedores de servicios separados, para reducir el riesgo de un tiempo de inactividad general en caso de un evento crítico.

d) Diseñar redes de datos con redundancia para asegurar la continuidad durante los fallos.

e) El almacenamiento de información debe realizarse en ubicaciones separadas geográficamente en el caso de los centros de datos.

f) Adquisición de sistemas alternos de electricidad que tengan la capacidad de lograr la redundancia según sea necesario.

Usar el balanceo de cargas y el fallo automático entre dos componentes o sistemas de software idénticos y redundantes para mejorar tanto el rendimiento en tiempo real como la resiliencia después de un evento crítico.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

Código	Ley, Política, Norma
19.00.001.2017	Lineamientos para el Funcionamiento del Modelo de Arquitectura de Información Empresarial para el Grupo ICE.

8.15 Registro

Deben producir, almacenar, proteger y analizar los registros que trazan las actividades, las excepciones, los fallos y otros eventos relevantes.

Propósito

Se requieren componentes de monitoreo y logging frecuentes para evaluar de manera efectiva los controles, las operaciones y la seguridad general de los sistemas de información del ICE.

Orientación

Los registros informáticos son esenciales para la gestión operativa de una organización. Proporcionan un mecanismo principal para el seguimiento y la generación de informes automatizados para las funciones de revisión, auditoría y cumplimiento, así como un mecanismo útil para el seguimiento de cambios y la resolución de problemas.

Este control aplica a todo el personal del ICE que crea, implementa o da soporte al software de aplicaciones y sistemas de información, los cuales se detallan a continuación:

a) El acceso a la red, los sistemas y las comunicaciones del ICE se registrará y supervisará para identificar posibles usos indebidos de los sistemas o la información. Las actividades de registro incluirán el monitoreo regular del acceso al sistema para evitar intentos de acceso no autorizado y confirmar que los sistemas de control de acceso sean efectivos. Los servidores de registro y los documentos se mantendrán seguros y solo estarán disponibles para el personal autorizado por el director de Ciberseguridad. Estos registros se mantendrán durante el tiempo que sea necesario o requerido para el uso funcional o la regulación o apropiada. Los sistemas de información del ICE (servidores, endpoint, firewalls, routers, switches, equipos de comunicaciones, etc.) se monitorearán y registrarán sus logs para:

- Asegurar que el uso está autorizado.
- Gestionar, administrar y resolver problemas de los sistemas.
- Proteger contra el acceso no autorizado.
- Verificar los procedimientos de seguridad y el acceso.
- Verificar el sistema y la seguridad operativa.

- Cumplir con la legislación, la normativa y lineamientos del ICE.
- Detectar y prevenir actividades delictivas o ilegales.

b) Los administradores de sistemas en el ICE implementarán logs de auditoría automatizados para todos los sistemas y componentes críticos. Como mínimo, los logs se utilizarán para reconstruir los siguientes eventos:
   - Accesos de usuarios individuales a sistemas e información confidencial.
   - Todas las acciones realizadas por cualquier individuo con privilegios administrativos.
   - Acceso a pistas de auditoría.
   - Intentos y fallas de acceso lógico no válido.
   - De uso y de cambios en los mecanismos de identificación y autenticación, incluidos, entre otros, la creación de nuevas cuentas y la elevación de privilegios, y todos los cambios, adiciones o eliminaciones de cuentas con privilegios administrativos.
   - Inicialización, detención o pausa de los registros de auditoría.
   - Creación y eliminación de objetos de nivel de sistema.

c) Todos los sistemas que manejan información confidencial aceptan conexiones de red o toman decisiones de control de acceso (autenticación y autorización) deben registrar y conservar la información de registro de auditoría para:
   - Determinar la actividad que se realizó.
   - Quién o qué realizó la actividad, incluido dónde o en qué sistema se realizó la actividad (sujeto).
   - Sistemas y objetos involucrados.
   - Cuando se realizó la actividad.
   - Estado (como éxito o fracaso), resultado, y/o resultado de la actividad.

d) Se asignará personal de apoyo para revisar y monitorear los registros de los sistemas cuando sea necesario. Los logs se revisarán de manera regular y continua. La frecuencia de revisión se determinará de acuerdo con la sensibilidad de la información almacenada, la función del sistema y otros requisitos del sistema según lo determine los administradores de los sistemas. Los procedimientos deben verificar que el registro esté activo y funcionando correctamente para:
   - Garantizar que los eventos se clasifiquen correctamente.
   - Revisar logs en busca de retrasos en el rendimiento.

- Asegurar que el registro relacionado con el cumplimiento no se pueda omitir.
- Verificar que el acceso a los archivos de logs esté correctamente restringido.
- Ayudar con las investigaciones.

e) Los logs se crearán cada vez que un sistema, una aplicación o un usuario realicen las siguientes actividades:
   - Crear, leer, actualizar o eliminar información confidencial, incluida la información de autenticación confidencial, como contraseñas.
   - Iniciar o aceptar una conexión de red.
   - Autenticar el acceso del usuario y autorizaciones de seguridad que este posea.
   - Otorgar, modificar o revocar derechos de acceso para incluir nuevas incorporaciones de usuarios o grupos, modificaciones de privilegios de usuarios, permisos de objetos de archivos o bases de datos, reglas de firewall y cambios de contraseñas de usuarios.
   - Configurar sistemas, redes o servicios para mantenimiento y cambios de seguridad, incluidos instalación de parches y actualizaciones de software, u otro software instalado.
   - Cambio de estado del inicio, apagado y/o reinicio de los procesos de las aplicaciones.
   - Cancelaciones, fallas o condiciones anormales de los procesos de las aplicaciones debido a límites o umbrales de recursos (como para CPU, memoria, ancho de banda de red, espacio en disco u otros recursos clave del sistema), falla del servicio de red, o fallas de hardware.
   - Detección de actividad sospechosa/maliciosa, como la de un IDS o IPS, un sistema antivirus o antispyware.

f) Las entradas de logs pueden contener una serie de elementos según el tipo y la función del sistema/proceso auditado. En general, las pistas de auditoría automatizadas incluirán la siguiente información:
   - Nombre del host, componente del sistema o recurso.
   - Sello de fecha/hora.
   - ID de la aplicación (por ejemplo, nombre y versión).
   - ID del proceso de inicio u origen del evento (por ejemplo, URL del punto de entrada, página, formulario).

- Ubicación del código (p. ej., módulo, subrutina).
- Usuario que inicia la acción (p. ej., ID de usuario).
- Tipo de evento.
- Estado del resultado (p. ej., correcto, fallido, diferido).
- Recurso (p. ej., identidad o nombre de los datos afectados, componente).
- Ubicación (p. ej. dirección IP o ubicación).
- Gravedad del evento (p. ej., emergencia, alerta, error fatal, advertencia, solamente informativo).

g) El sistema admitirá el formateo y el almacenamiento de registros de auditoría para garantizar la integridad del análisis y la generación de informes a nivel empresarial. Los mecanismos conocidos para respaldar estos objetivos incluyen, entre otros, los siguientes enfoques:

- Recopilación de logs de eventos de Microsoft Windows de los servidores mediante un sistema de administración de logs centralizado.
- Almacenamiento de logs en un formato documentado y enviado a través de una red con protocolos confiables a un sistema de administración de logs centralizado.
- Almacenamiento de entradas de logs en una base de datos SQL que genera registros de auditoría de conformidad con los requisitos de estos controles.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
19.00.001.2017	Lineamientos para el Funcionamiento del Modelo de Arquitectura de Información Empresarial para el Grupo ICE.

8.16 Actividades de seguimiento

Las redes, los sistemas y las aplicaciones deben supervisarse para detectar comportamientos anómalos y tomar las medidas adecuadas para evaluar posibles incidentes de seguridad de la información.

Propósito

Detectar comportamientos anómalos y posibles incidentes de seguridad de la información.

Orientación

El alcance y el nivel de la supervisión deben determinarse de acuerdo con los requisitos de la institución y de seguridad de la información; teniendo en cuenta las leyes y reglamentos correspondientes. Los registros de supervisión deben mantenerse durante períodos de conservación definidos.

Las siguientes tareas son recomendadas para la consecución del propósito:

a) Identificar y revisar los incidentes e intentos de violación a la seguridad de la información, tanto los que tuvieron éxito como los que fracasaron.

b) Posibilitar que la Dirección Ciberseguridad determine si las actividades de seguridad delegadas a las personas o implementadas mediante tecnología de la información se están ejecutando en la forma esperada.

c) Ayudar a detectar eventos de seguridad, y de esta manera impedir incidentes de seguridad mediante el uso de indicadores.

d) Determinar si las acciones tomadas para solucionar un problema de violación a la seguridad fueron eficaces.

e) Realizar revisiones regulares que incluyan el cumplimiento de la normativa y objetivos de seguridad de la Información, y la revisión de los controles de seguridad, teniendo en cuenta los resultados de las auditorías de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas.

f) Medir la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad de la información definidos por la institución.

g) Revisar la valoración de los riesgos a intervalos planificados, y revisar el nivel de riesgo residual y riesgo aceptable identificado, teniendo en cuenta los cambios en la institución, la tecnología, los objetivos y procesos, las amenazas identificadas, la eficacia de los controles implementados, eventos externos (como cambios en el entorno legal o reglamentario, en las obligaciones contractuales, y en el clima social).

h) Ejecutar acciones correctivas y preventivas adecuadas, aplicando las lecciones aprendidas de las experiencias de seguridad de la información ante la atención de incidentes de seguridad.

i) Comunicar las acciones y mejoras a las partes interesadas que corresponda, con un nivel detalle apropiado a las circunstancias y en donde sea pertinente, llegar a acuerdos sobre cómo proceder.

j) Asegurar que las mejoras logran los objetivos previstos.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

8.17 Sincronización del reloj

Los relojes de los sistemas de procesamiento de información utilizados por ICE deben estar sincronizados con las fuentes de tiempo aprobadas y oficializadas.

Propósito

Permitir la correlación y el análisis de los eventos relacionados con la seguridad y otros datos registrados, y apoyar las investigaciones sobre incidentes de seguridad de la información.

Orientación

Los requisitos externos e internos para la representación del tiempo, la sincronización fiable y la precisión deben documentarse y aplicarse.

Dichos requisitos pueden provenir de necesidades legales, reglamentarias, contractuales, normativas y de control interno.

Debe definirse y considerarse una hora de referencia para su uso dentro de la Institución, para todos los sistemas, incluidos los sistemas de gestión de edificios, los sistemas de entrada y salida y otros que puedan utilizarse para ayudar en las investigaciones.

La configuración correcta de los relojes de los ordenadores es importante para garantizar la exactitud de los registros de eventos, que pueden ser necesarios para las investigaciones o como prueba en casos judiciales y/o disciplinarios.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

8.18 Uso de programas de utilidad privilegiados

El uso de programas de utilidad que pueden ser capaces de anular los controles del sistema y de la aplicación debe ser restringido y controlado estrictamente.

Propósito

Garantizar que el uso de programas de utilidad no perjudique los controles del sistema y de las aplicaciones para la seguridad de la información.

Orientación

Deben tenerse en cuenta los siguientes controles para el uso de programas de utilidad que pueden ser capaces de anular los controles del sistema y de la aplicación:

a) Limitación del uso de los programas de utilidad al mínimo número práctico de usuarios autorizados y de confianza.
b) Uso de procedimientos de identificación, autentificación y autorización para los programas de utilidad, incluyendo la identificación única de la persona que utiliza el programa.
c) Definir y documentar los niveles de autorización de los programas de utilidad.
d) Autorización para el uso ad hoc de programas de utilidad.
e) No poner los programas de utilidad a disposición de los usuarios que tienen acceso a las aplicaciones en los sistemas en los que se requiere la segregación de funciones.
f) Eliminar o desactivar todos los programas de utilidad innecesarios.
g) Como mínimo, la segregación lógica de los programas de utilidad del software de aplicación. Cuando sea práctico, segregar las comunicaciones de red para dichos programas del tráfico de aplicaciones.
h) Limitación de la disponibilidad de los programas de utilidad (por ejemplo, durante la duración de un cambio autorizado).

i) Registro de todo el uso de los programas de utilidad.

En el ICE existen gran cantidad de programas de utilidad que pueden ser capaces de anular los controles de un sistema y de las aplicaciones, por ejemplo, diagnósticos, parches, antivirus, desfragmentadores de disco, depuradores, copias de seguridad y herramientas de red.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.

8.19 Instalación de software en los sistemas operativos

Deben implementarse procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.

Propósito

Garantizar la integridad de los sistemas operativos y evitar la explotación de las vulnerabilidades técnicas.

Orientación

Se deben tener en cuenta los siguientes controles para gestionar de forma segura los cambios y la instalación de software en los sistemas operativos:

a) Realizar las actualizaciones del software operativo sólo por parte de administradores capacitados y con la debida autorización del titular subordinado correspondiente.

b) Garantizar que sólo se instala en los sistemas operativos el código ejecutable aprobado y ningún código de desarrollo o compilador.

c) Sólo instalar y actualizar el software después de haber realizado pruebas exhaustivas y satisfactorias (ver 8.29 y 8.31).

d) Actualizar todas las bibliotecas de fuentes de programas correspondientes.

e) Utilizar un sistema de control de la configuración para mantener el control de todo el software operativo, así como la documentación del sistema.

f) Definir una estrategia de reversión antes de aplicar los cambios.

g) Mantener un registro de auditoría de todas las actualizaciones del software operativo;

h) Archivar las versiones antiguas de los programas informáticos, junto con toda la información y los parámetros necesarios, los procedimientos, los detalles de la configuración y los programas informáticos de apoyo como medida de contingencia, y durante todo el tiempo que el programa informático deba leer o procesar los datos archivados.

Para el ICE es importante mantener procedimientos para cubrir las instalaciones de Software en cualquier dispositivo dentro de una organización. Estos procedimientos deben fijarse en la aplicabilidad de los siguientes controles:

a) Probar las nuevas aplicaciones o software en entornos aislados especialmente preparados para pruebas.

b) Comprobar las necesidades de instalación (compatibilidad del entorno) antes de su instalación.

c) Valorar la necesidad de actualización o instalación.

d) Planificar la forma de volver a versiones anteriores en caso de ser necesario.

e) Los entornos de desarrollo y pruebas deben permanecer aislados de los entornos operativos.

f) Las instalaciones de software deben ser realizada por usuarios autorizados.

g) Establecer procedimientos o herramientas de monitoreo del software para detectar cambios no autorizados.

h) Las pruebas posteriores a la implementación deben incluir una supervisión de la red para identificar cualquier tráfico inesperado que pueda exponer errores o suponga empeoramiento de la velocidad de las transmisiones.

A la vez se debe de insistir en establecer restricciones para la instalación de software por parte de los usuarios y que toda instalación de software debe realizarse por personal autorizado y con la capacitación adecuada. Aquí se trata de que además se definan unas reglas concisas para limitar la capacidad de los usuarios finales.

Estas restricciones deben ir enfocadas a identificar expresamente:

a) Qué tipos de instalaciones de software son las permitidas a los usuarios finales (por ejemplo, actualizaciones y parches de seguridad al software existente).

b) Qué tipos de instalaciones de software se encuentran prohibidas (por ejemplo, software que es sólo para uso personal y software cuyo origen pueda ser potencialmente dañino etc.).

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.

8.20 Seguridad de las redes

Las redes y los dispositivos de red deben estar asegurados, gestionados y controlados para proteger la información de los sistemas y las aplicaciones.

Propósito

Proteger la información en las redes y sus instalaciones de procesamiento de información de apoyo contra el compromiso a través de la red.

Orientación

Deben implementarse controles para garantizar la seguridad de la información en las redes y para proteger los servicios conectados del acceso no autorizado según las posibilidades de la infraestructura involucrada. En particular, deben tenerse en cuenta los siguientes elementos:

a) El tipo y el nivel de clasificación de la información que puede soportar la red.
b) Establecer responsabilidades y procedimientos para la gestión de los equipos y dispositivos de red.
c) Mantener la documentación actualizada, incluidos los diagramas de red y los archivos de configuración de los dispositivos.
d) Separar la responsabilidad operativa de las redes de las operaciones de los sistemas.

e) Establecer controles para salvaguardar la confidencialidad e integridad de los datos que pasan por las redes públicas, las redes de terceros o por las redes inalámbricas y para proteger los sistemas y aplicaciones conectados. Deben generarse controles adicionales para mantener la disponibilidad de los servicios de red y de los ordenadores conectados a la red.

f) Registrar y supervisar adecuadamente para permitir el registro y la detección de acciones que puedan afectar a la seguridad de la información o que sean relevantes para ella.

g) Coordinar estrechamente las actividades de gestión de la red tanto para optimizar el servicio a la Institución, como para garantizar que los controles se aplican de forma coherente en toda la infraestructura de procesamiento de la información.

h) Autentificar los sistemas en la red.

i) Restringir y filtrar la conexión de los sistemas a la red.

j) Detectar, restringir y autentificar la conexión de equipos y dispositivos a la red.

k) Asegurar los dispositivos de red mediante la reducción de sus vulnerabilidades.

l) Segregar los canales de administración de la red del resto del tráfico de la red.

m) Aislar temporalmente las subredes críticas si la red está siendo atacada.

n) Desactivar los protocolos de red vulnerables.

o) Asegurar de que se aplican los controles de seguridad adecuados al uso de las redes virtualizadas. las redes virtualizadas también abarcan las redes definidas por software (SDN, SD-WAN).

p) La configuración de los componentes de la red cumplirá como mínimo con lo estipulado en las líneas base de seguridad respectiva.

q) Se establecerá e implementará un programa de mantenimiento periódico de los componentes de la red, el cual debe considerar las recomendaciones que señale el fabricante cuando corresponda.

r) La Institución, establecerá mecanismos de cifrado de información que proporcionen integridad y confidencialidad a la información que transporta la red interna que por su sensibilidad lo requiera.

s) La Institución, establecerá un mecanismo de administración de nodos para evitar puntos de acceso no controlados.

t) En la medida de lo posible para ingresar a los servicios de la red interna de la Institución, se debe contar con un mecanismo de administración de identidad basado en roles de acuerdo con control de acceso a dichos servicios.

u) La red interna de la empresa estará segmentada.

v) Se contará con segmentos de red seguros (Zona Desmilitarizada, DMZ por sus siglas en inglés) donde sea requerido para asegurar el acceso a la red interna.

w) El segmento de la red interna en donde se encuentran ubicadas las estaciones de administración y monitoreo, serán independientes de la red de datos de usuarios y de las actividades relacionadas con la operación de la Empresa.

x) La seguridad de la red interna contemplará las medidas y controles que permitan complementar la seguridad de los servicios de tecnologías de información (correo, sistemas de información, acceso a Internet, entre otros).

y) Se deberán llevar a cabo análisis de riesgos de seguridad de la información sobre la red interna de la empresa de forma periódica para detectar las posibles vulnerabilidades y amenazas con el fin de reducir la probabilidad de ocurrencia de éstos.

Protección de conexión a redes externas

La institución, establecerá controles de seguridad en la infraestructura que soporta las conexiones entre las redes externas y la red interna enfocados en la confidencialidad, integridad y disponibilidad de la información que transportan, con el fin de asegurar la protección de la información empresarial. Establecerá un inventario de todas las conexiones entre la red interna y redes externas.

Las nuevas conexiones externas que se requieran implementar deberán basarse en la normativa interna establecida en ICE.

La Gerencia Tecnología y Soluciones Digitales, es la encargada de la gestión de las redes internas y son los responsables de establecer los controles técnicos específicos de arquitectura, configuraciones, procedimientos y guías para la seguridad de las conexiones externas para la preservación de la confidencialidad, integridad y disponibilidad de la información.

Las conexiones con terceros contarán con el contrato y autorizaciones pertinentes.

Los incidentes de seguridad de la información relacionados con conexiones a las redes externas serán registrados y notificados.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.

Código	Ley, Política, Norma
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.
87.00.001.2023	Política de Seguridad de Redes de Comunicaciones.
GU-GTSD-SC-SI-001	Guia Mejores Prácticas Ciberseguridad Redes TI
GU-GTSD-SC-SI-003	Guia Mejores Prácticas Ciberseguridad Redes TO

8.21 Seguridad de los servicios de red

Los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red deben ser identificados, implementados y supervisados.

Propósito

Garantizar la seguridad en el uso de los servicios de red.

Orientación

Las medidas de seguridad necesarias para determinados servicios, como las características de seguridad, los niveles de servicio y los requisitos de servicio, deben ser identificadas e implementadas. La Institución, debe asegurarse de que los proveedores de servicios de red apliquen estas medidas.

La capacidad del proveedor de servicios de red para gestionar los servicios acordados de forma segura debe determinarse y supervisarse regularmente. El derecho a la auditoría debe acordarse entre la institución y el proveedor. La Institución también debería considerar las certificaciones de terceros proporcionadas por los proveedores de servicios para demostrar que mantienen las medidas de seguridad adecuadas.

Deben formularse y aplicarse normas sobre el uso de las redes y los servicios de red para cubrir:

a) Las redes y los servicios de red a los que se puede acceder.
b) Los requisitos de autenticación para acceder a los distintos servicios de la red;
c) procedimientos de autorización para determinar quién puede acceder a qué redes y servicios en red.

d) La gestión de la red y los controles y procedimientos tecnológicos para proteger el acceso a las conexiones y servicios de la red.

e) Los medios utilizados para acceder a las redes y a los servicios de red.

f) Hora, ubicación y otros atributos del usuario en el momento del acceso.

g) La supervisión del uso de los servicios de la red.

Se deberán tener en cuenta las siguientes características de seguridad de los servicios de red:

a) Tecnología aplicada para la seguridad de los servicios de red, como la autenticación, la codificación y los controles de conexión a la red.

b) Los parámetros técnicos necesarios para la conexión segura con los servicios de la red de acuerdo con las normas de seguridad y de conexión a la red.

c) El almacenamiento en caché y sus parámetros que permiten a los usuarios elegir el uso de la caché de acuerdo con los requisitos de rendimiento, disponibilidad y confidencialidad.

d) Procedimientos para el uso del servicio de red para restringir el acceso a los servicios o aplicaciones de la red, cuando sea necesario.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.
87.00.001.2023	Política de Seguridad de Redes de Comunicaciones.
GU-GTSD-SC-SI-001	Guia Mejores Prácticas Ciberseguridad Redes TI
GU-GTSD-SC-SI-003	Guia Mejores Prácticas Ciberseguridad Redes TO

8.22 Segregación de redes

Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en las redes de la institución.

Propósito

Dividir la red en límites de seguridad y controlar el tráfico entre ellos en función de las necesidades de negocio.

Orientación

La institución debe considerar la posibilidad de gestionar la seguridad de las grandes redes dividiéndolas en dominios de red independientes y separándolas de la red pública (es decir, Internet). Los dominios pueden elegirse en función de los niveles de confianza, criticidad y sensibilidad (por ejemplo, dominio de acceso público, dominio de escritorio, dominio de servidor, sistemas de bajo y alto riesgo), a lo largo de las unidades organizacionales (por ejemplo, recursos humanos, finanzas, marketing) o alguna combinación (por ejemplo, dominio de servidor que se conecte a múltiples unidades organizacionales). La segregación puede hacerse utilizando redes físicamente diferentes o utilizando redes lógicas diferentes.

Para el ICE es de suma importancia poder mantener estas segregaciones bien marcadas y controladas dada la gran variedad de tráfico, la criticidad de la información y la demanda de calidad en el transporte.

Las redes inalámbricas son particularmente vulnerables con respecto a la seguridad y esto debe considerarse como parte de la estrategia de segregación.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.
87.00.001.2023	Política de Seguridad de Redes de Comunicaciones.

Código	Ley, Política, Norma
GU-GTSD-SC-SI-001	Guia Mejores Prácticas Ciberseguridad Redes TI
GU-GTSD-SC-SI-003	Guia Mejores Prácticas Ciberseguridad Redes TO

8.23 Filtrado web

El acceso a sitios web externos debe ser gestionado para reducir la exposición a contenidos maliciosos.

Propósito

Definir controles de buen uso del internet, con el fin de asegurar una adecuada protección de la información del ICE, con el fin de proteger los sistemas para evitar que sean comprometidos por el programa maligno, así mismo, para prevenir el acceso a recursos web no autorizados.

Orientación

Propiciar los mecanismos para reducir los riesgos de que los usuarios (funcionarios y terceros) accedan a sitios web que contengan información ilegal o que contienen virus o material de Phishing, spyware y otro tipo de software o código malicioso, con base a la *“Política de Seguridad de Redes de Comunicaciones”.*

A continuación, se detallan los controles de seguridad para su implementación:

a) El acceso a internet básico de acuerdo con las posibilidades institucionales se suministrará a todos los funcionarios y trabajadores del ICE que lo requieran para el cumplimiento de sus funciones.

b) La Dirección de Soluciones Tecnológicas, como administrador de los servicios de comunicación, establecerá los controles que permitan regular el buen uso del acceso a internet y restringir el acceso a sitios que contravengan la legislación vigente y las normativas institucionales. De igual manera establecerá los controles que permitan garantizar la buena operación del servicio.

c) La autorización de acceso a sitios en internet para los cuales existe alguna regulación o restricción establecida por la institución debe ser tramitada con la autorización del Titular Subordinado por medio de la mesa de ayuda al Centro de Soporte de Usuario Final (CSUF).

d) Está prohibido acceder al servicio de internet, desde equipos conectados a la red institucional, a través de servidores ajenos a la institución, indistintamente del medio de comunicación que se emplee para tal fin: conexión remota telefónica,

conexión inalámbrica (Wireless), banda ancha (ADSL, RDSI), o cualquier otro medio.

e) Incluir el uso de firewalls para filtrado de tráfico no deseado.

f) Los administradores de la red contarán e implementarán sistemas de filtrado de contenido para la óptima operación de la red de la Empresa.

g) Un filtro corporativo de Internet se utiliza para prevenir tipos específicos de sitios web que se accede. Si un usuario necesita acceder a un sitio web que está bloqueado o restringido, el jefe inmediato debe solicitar por los canales de comunicación establecidos, la respectiva autorización a la Gerencia Tecnología y Soluciones Digitales.

h) Todo usuario es responsable de informar el acceso a contenidos o servicios no autorizados o que no correspondan al desempeño de sus funciones o actividades dentro de la institución. Todos los usuarios son responsables del uso de sus credenciales de acceso a las cuales les fue otorgado el acceso a internet.

i) Todos los usuarios que se encuentren autorizados son responsables de dar un uso adecuado de este recurso y por ninguna razón pueden hacer uso para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente, las normativas de seguridad de la información, la seguridad de la información, entre otros.

j) Todos los usuarios invitados que requieran acceso a internet dentro de las instalaciones del ICE deben realizarlo por medio de la red WIFI invitados y cumplir con los requerimientos que el portal solicita, una vez que tengan acceso al servicio de internet, deben cumplir estrictamente con las normativas de seguridad de la información, de lo contrario asumirán las acciones pertinentes.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.

Código	Ley, Política, Norma
87.00.001.2023	Política de Seguridad de Redes de Comunicaciones.
GU-GTSD-SC-SI-001	Guia Mejores Prácticas Ciberseguridad Redes TI
GU-GTSD-SC-SI-003	Guia Mejores Prácticas Ciberseguridad Redes TO

8.24 Uso de la criptografía

Deben definir y aplicar normas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.

Propósito

Garantizar la implementación y eficaz de la criptografía para proteger la confidencialidad, la autenticidad o la integridad de la información.

Orientación

La institución debe establecer una normativa específica sobre criptografía, en la cual se consideren los principios generales para la protección de la información.

El ICE desarrollará los procedimientos adecuados necesarios en torno al uso de controles criptográficos. Se deben considerar los siguientes elementos:

a) Con base en una evaluación de riesgos, se debe identificar el nivel de protección requerido considerando el tipo, la fuerza y la calidad del algoritmo de cifrado requerido.

b) El uso de cifrado para la protección de la información trasegada de forma interna o externa por dispositivos móviles, medios extraíbles o líneas de comunicación.

c) Las claves criptográficas deben protegerse durante todo su ciclo de vida, contra modificaciones y pérdidas; además de protección adicional contra el uso no autorizado o divulgación.

d) Los algoritmos criptográficos, las longitudes de clave y las prácticas de uso deben seleccionarse de acuerdo con las mejores prácticas.

e) El equipo utilizado para generar, almacenar y archivar claves debe protegerse físicamente.

f) Debe considerarse la normativa vigente, las regulaciones y restricciones para el uso y aplicación de las técnicas criptográficas.

g) En caso de generarse acuerdos de nivel de servicio o de contratos con proveedores externos de servicios criptográficos, estos deben considerar los aspectos de responsabilidad y seguridad de la información necesarios.

Para que se dé una adecuada gestión de las claves se requieren procesos seguros para generar, almacenar, archivar, recuperar, distribuir, retirar y eliminar las claves criptográficas.

Un sistema de gestión de claves debe basarse en un conjunto acordado de normas, procedimientos y métodos seguros.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.
Código pendiente de Asignación	Política de Seguridad de Redes de Comunicaciones.
19.00.001.2017	Lineamientos para el Funcionamiento del Modelo de Arquitectura de Información Empresarial para el Grupo ICE.
GU-GTSD-SC-SI-001	Guia Mejores Prácticas Ciberseguridad Redes TI
GU-GTSD-SC-SI-003	Guia Mejores Prácticas Ciberseguridad Redes TO

8.25 Ciclo de vida de desarrollo seguro

Deben establecerse y aplicarse normas para el desarrollo seguro de software y sistemas.

Propósito

Este control define los requisitos de alto nivel para proporcionar orientación a los administradores de programas comerciales, administradores de proyectos comerciales,

administradores de proyectos técnicos y otras partes interesadas de programas y proyectos para respaldar la aprobación, la planificación y el desarrollo del ciclo de vida de los sistemas de software del ICE.

Orientación

El control de ciclo de vida de desarrollo seguro se aplica a las personas que participan en el desarrollo de cualquier Activo de Información del ICE, como se indica a continuación:

a) Las aplicaciones creadas o implementadas dentro del entorno de TI del ICE deben seguir un ciclo de vida de aplicación estandarizado establecido por la administración.

b) Las aplicaciones deben mantenerse activamente y tener actualizaciones periódicas para abordar las vulnerabilidades. Si el desarrollador u otra parte ya no mantiene una aplicación, debe evaluarse para reemplazarla.

c) Al inicio de la fase de adquisición o diseño de la implementación de una aplicación, el responsable de seguridad debe proporcionar una lista de los controles de seguridad necesarios según el estándar de ciclo de vida de desarrollo de software seguro.

d) Los entornos de desarrollo, pruebas y operativos deben estar separados.

e) Debe existir una separación de funciones entre el personal asignado a los entornos de desarrollo/prueba y el asignado al entorno de producción.

f) Los cambios en el sistema deben realizarse de acuerdo con el control de cambios.

g) Cuando se cambian las plataformas operativas, las aplicaciones críticas para el negocio deben revisarse y probarse para garantizar que no haya un impacto adverso en las operaciones o la seguridad de la institución.

h) La fuente de datos de producción debe cuidadosamente revisada antes de su uso en un entorno de desarrollo o prueba y los controles de acceso de producción/prueba deben cumplir con los estándares de producción.

i) Los datos de prueba y las cuentas deben eliminarse antes de que un sistema de producción se active.

j) Todo el personal de desarrollo de software debe recibir capacitación en la escritura de código seguro para su entorno de desarrollo específico.

k) Se debe desarrollar e implementar un estándar de ciclo de vida de desarrollo de software seguro.

l) El acceso al código fuente del programa debe estar restringido según el principio de mínimo privilegio.

m) Para las aplicaciones que almacenan o transmiten información confidencial, se deben implementar controles para limitar la salida al mínimo necesario según lo definido por el usuario.

n) Cualquier desarrollo de software contratado debe cumplir con las recomendaciones del estándar de ciclo de vida de desarrollo de software seguro.

o) Las modificaciones a los paquetes de software desarrollados externamente deben limitarse a los cambios necesarios y todos los cambios deben controlarse estrictamente.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

8.26 Requisitos de seguridad de la aplicación

Los requisitos de seguridad de la información deben ser identificados, especificados y aprobados cuando se desarrollen o adquieran aplicaciones.

Propósito

Garantizar que todos los requisitos de seguridad de la información se identifiquen y aborden al desarrollar o adquirir aplicaciones.

Orientación

Deben identificarse y especificarse los requisitos de seguridad de las aplicaciones. Estos requisitos generalmente se determinan a través de una evaluación de riesgos. Los requisitos deben desarrollarse con el apoyo de especialistas en seguridad de la información.

Los requisitos de seguridad de la aplicación pueden cubrir una amplia gama de temas, según el propósito de la aplicación por medio de los siguientes pasos:

a) Crear modelo de aplicación, el equipo de desarrollo debe concentrarse en crear la aplicación y obtener la aprobación de la administración y el Proceso Seguridad de la Información.

b) Se debe asegurar que el sistema de autenticación de la aplicación esté actualizado.

c) Se debe utilizar autenticación de dos factores, de modo que los usuarios no solo deban ingresar una contraseña, sino también un código enviado al número de teléfono o correo electrónico adjunto a su cuenta para ingresar.

d) El siguiente paso es asegura de que el sistema de autenticación de las aplicaciones esté actualizado.

e) Asegurarse que nadie, excepto los usuarios administrativos, tengan acceso a los directorios y archivos de la aplicación.

f) Implementar el tiempo de espera de vencimiento de la sesión.

g) Se debe prohibir varias sesiones simultáneas:

- Establecer una bandera en el momento de iniciar sesión en la base de datos.
- Verifique la bandera cada vez que inicie sesión.
- Eliminar bandera al momento de cerrar sesión.

h) Proporcionar privilegios mínimos a los usuarios de las aplicaciones: esto significa que todos los usuarios solo deben tener acceso a lo que absolutamente necesitan y nada más que eso.

i) Implementar CAPTCHA y el sistema de verificación de correo electrónico

- CAPTCHA y la verificación de correo electrónico tienen diferentes propósitos, pero ambos son igualmente importantes.
- CAPTCHA se asegura de que sean personas reales las que envían formularios y no scripts.
- La verificación de correo electrónico garantiza que la dirección de correo electrónico que se ingresó realmente existe y funciona.

j) Dependiendo de los requerimientos y la sensibilidad de la información de las aplicaciones institucionales, es necesario que se realicen las evaluaciones para utilizar las mejores opciones de algoritmos de cifrado de datos.

k) Las API son las claves de las bases de datos de una empresa, por lo que es muy importante restringir y monitorear quién tiene acceso a ellas.

l) Se deben ejecutar auditorías de seguridad en los códigos fuente.

m) Realizar escaneos de vulnerabilidad de aplicaciones web es sumamente importante para la institución.

n) Se deben de realizar pruebas de penetración.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

8.27 Arquitectura de sistemas seguros y principios de ingeniería

Los principios para la ingeniería de sistemas seguros deben establecerse, documentarse, mantenerse y aplicarse a cualquier actividad de desarrollo de sistemas de información.

Propósito

Garantizar que los sistemas de información en el ICE se diseñen, implementen y operen de forma segura dentro del ciclo de vida del desarrollo.

Orientación

Los principios de ingeniería de seguridad deben establecerse, documentarse y aplicarse a las actividades de ingeniería de sistemas de información. La seguridad debe diseñarse en todas las capas de la arquitectura (negocios, datos, aplicaciones y tecnología). La nueva tecnología debe analizarse en busca de riesgos de seguridad y el diseño debe revisarse frente a patrones de ataque conocidos.

Los principios de ingeniería segura brindan orientación sobre las técnicas de autenticación de usuarios, el control seguro de sesiones y la validación y desinfección de datos, los cuales se detallan a continuación:

a) Establecer una política de seguridad de la información sólida como la “base” para el diseño.
b) Tratar la seguridad como parte integral del diseño del sistema.
c) Delinear claramente los límites de seguridad físicos y lógicos que se rigen por las normas de seguridad asociadas.
d) Los desarrolladores deben estar capacitados para desarrollar software seguro.
e) Reducir el riesgo a un nivel óptimo.
f) Asumir que los sistemas externos son inseguros.
g) Identificar las compensaciones potenciales entre la reducción del riesgo y el aumento de los costos y la disminución de otros aspectos de la eficacia operativa.

h) Implementar medidas de seguridad del sistema personalizadas para cumplir con los objetivos de seguridad de la institución.
i) Proteger la información mientras se procesa, se transporta y se almacena.
j) Considerar productos a la medida para lograr una seguridad adecuada.
k) Protegerse contra todas las clases probables de "ataques".
l) Siempre que sea posible, base la seguridad en estándares abiertos para la portabilidad y la interoperabilidad.
m) Usar un lenguaje común en el desarrollo de requisitos de seguridad.
n) Diseñar la seguridad para permitir la adopción regular de nueva tecnología, incluido un proceso de actualización de tecnología seguro y lógico.
o) Esforzarse por la facilidad de uso operativo.
p) Implementar seguridad en capas.
q) Proporcionar garantías de que el sistema es y sigue siendo resistente frente a las amenazas previstas.
r) Limitar o contener vulnerabilidades.
s) Aísle los sistemas de acceso público de los recursos de misión crítica.
t) Usar mecanismos de límites para separar los sistemas informáticos y las infraestructuras de red.
u) Diseñar e implementar mecanismos de auditoría para detectar el uso no autorizado y apoyar las investigaciones de incidentes.
v) Desarrollar y poner en práctica procedimientos de contingencia o recuperación ante desastres para garantizar la disponibilidad adecuada.
w) Implementar privilegios mínimos.
x) No implementar mecanismos de seguridad innecesarios.
y) Garantizar la debida seguridad en la parada o enajenación de un sistema.
z) Identifique y prevenga errores y vulnerabilidades comunes.
aa) Implementar la seguridad a través de una combinación de medidas distribuidas física y lógicamente.
bb) Formular medidas de seguridad para abordar múltiples dominios de información superpuestos.
cc) Autenticar usuarios y procesos para garantizar decisiones de control de acceso adecuadas tanto dentro como entre dominios.
dd) Utilice identidades únicas para garantizar la responsabilidad.
ee) Considere los principios de Zero Trust de la NIST.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

8.28 Desarrollo seguro de software

Los principios de desarrollo seguro de software deben aplicarse como un modelo de trabajo basado en revisiones de seguridad continuas, durante el ciclo de vida del desarrollo de software.

Se deben implementar umbrales de seguridad en varios o todos los siguientes ámbitos:

a) Algoritmos de programación.
b) Composición de dependencias.
c) Tecnologías de contenedores.
d) Infraestructura como código (nube).
e) Proceso de entrega continua.

Propósito

El propósito de este control es definir las reglas básicas para desarrollo seguro de software y sistemas del ICE.

Orientación

El alcance y enfoque del control de desarrollo seguro incluye las actividades del ciclo de vida de desarrollo de software y mantenimiento de aplicaciones de los servicios, arquitectura, y sistemas que forman parte de los negocios del ICE.

Los custodios de la información son los responsables de proporcionar respaldos de seguridad adecuadas para garantizar la recuperación de la información electrónica en caso de falla. Estas disposiciones de respaldo permitirán que los procesos críticos del ICE se reanuden en un período de tiempo razonable con una pérdida mínima de datos. Dado que las fallas pueden tomar muchas formas y pueden ocurrir con el tiempo, se deben mantener múltiples instancias de respaldos de seguridad, las cuales se mencionan a continuación:

a) Se deben evaluar los riesgos relacionados con:

- El acceso no autorizado al ambiente de desarrollo.
- Los cambios no autorizados sobre el ambiente de desarrollo.
- Las vulnerabilidades técnicas de los sistemas de TI utilizados en la institución.
- Los riesgos que puede traer una nueva tecnología si se utiliza en la institución.

b) Asegurar que los desarrollos cumplan con lo estipulado en DevSecOps.

c) Usar técnicas de programación seguras tanto para nuevos desarrollos, y en caso de reutilización de código, asegurarse que siga las buenas prácticas actuales de OWASP TOP 10.

d) Tener una arquitectura de la aplicación que contemple controles de diseño seguro.

e) Diseñar un diagrama de infraestructura para administrar adecuadamente los cambios, mejoras y/o problemas que pudieran surgir en la infraestructura tecnológica.

f) Documentar la estructura de la base de datos, sus tablas y los algoritmos de cifrado que se utilizan en ella.

g) Tener documentación sobre cómo instalar (herramienta o método de revisión de código) en el IDE del desarrollador para verificaciones de estilos comunes.

h) Documentar los resultados y la ejecución de pruebas de seguridad.

i) Desarrollo de Servicios y Acciones Masivas.

j) Desarrollos de Front End.

k) El almacenamiento de claves debe de estar protegido y estas claves se encuentran hasheadas mediante el protocolo así definido por la institución.

l) Los integrantes del equipo deben utilizar un gestor de contraseñas robusto.

m) Los integrantes del equipo no deben compartir contraseñas, si un miembro del equipo requiere un usuario y/o contraseña para acceder a un servicio, el mismo debe solicitarlo al titular subordinado, el cual se encargará de darle los accesos solicitados.

n) En el caso de contar con desarrollo externalizado, convenir con el proveedor los requisitos de desarrollo seguro que podrán ser auditados para evaluar a los proveedores de forma colaborativa.

o) Se deben establecer condiciones contractuales por parte del proveedor para desarrollos externalizados, para resguardar la propiedad intelectual de la empresa y asegurar la total confidencialidad de su información y de sus clientes.

p) Segmentar los ambientes, es decir, contar con ambientes de desarrollo, prueba y producción.

q) Garantizar que los ambientes no compartan la misma red, base de datos ni claves.

r) El tráfico entrante a los ambientes se restringe mediante firewall de red interna, un firewall de externo y un Web Application Firewall.

s) Cualquier ambiente de desarrollo estará protegido con restricción de acceso exclusivo al personal autorizado por la Gerencia Tecnología y Soluciones Digitales.

t) Contar con repositorios en los cuales se restrinja su acceso, grupo de seguridad en entorno CI/CD. A su vez, se debe asegurar que al código fuente se le aplique:

- Control y trazabilidad de código.
- Código salvaguardado y recuperable.
- Seguimiento a los controles del template de merge donde se incluye: problemas relacionados, descripción del problema, motivo del cambio, capturas de pantalla (si tiene cambios visuales), pasos para probar el correcto funcionamiento de los cambios, checklist con puntos que deben cumplirse.

u) Contar con aprobaciones de los líderes de producto para los pases a producción.

v) Manejo de versiones de los proyectos de desarrollo.

w) Asignar planes de capacitación para que el equipo tenga capacidad y conocimiento para:

- Conocer y evaluar condiciones de seguridad de los desarrollos.
- Evitar, detectar y resolver incidentes y vulnerabilidades.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

8.29 Pruebas de seguridad en el desarrollo y la aceptación

Los procesos de pruebas de seguridad deben definirse e implementarse en el ciclo de vida del desarrollo.

Propósito

El propósito de este control es establecer las reglas para evaluar, desarrollar y/o desplegar Recursos de Información.

Orientación

Los nuevos sistemas de información, las actualizaciones y las nuevas versiones deben probarse y verificarse minuciosamente durante los procesos de desarrollo. Las pruebas de seguridad deben ser una parte integral de las pruebas de sistemas o componentes.

Las pruebas de seguridad deberían enfocarse en lo siguiente:

a) Seguridad de la red: búsqueda de vulnerabilidades en la infraestructura de la red, incluidos los recursos y las normativas correspondientes.

b) Seguridad del software del sistema: evaluación de las debilidades en los diversos softwares de los que depende la aplicación, incluido el sistema operativo y el sistema de base de datos.

c) Seguridad de la aplicación del lado del cliente: garantizar que el cliente no pueda ser manipulado a través de un navegador o cualquier otra herramienta.

d) Seguridad de la aplicación del lado del servidor: garantizar que el código del servidor sea lo suficientemente robusto como para evitar intentos de intrusión.

e) Seguridad del código: Comprobar del código fuente de la aplicación para identificar y eliminar vulnerabilidades durante el desarrollo y garantizar la "mantenibilidad a largo plazo" del código. Implica comprobaciones de muchos aspectos, entre ellos:

- Autenticación
- Autorización
- Validación de datos
- Manejo de errores
- Gestión de sesiones
- Configuración de seguridad
- Inicio sesión
- Cifrado

f) Los criterios de aceptación deben ser proporcionados por el propietario de la aplicación y deben especificar:

- Los requisitos operativos y funcionales de la aplicación.

- Requisitos de rendimiento y capacidad.
- Todos los criterios de aceptación deben cumplirse antes de que cualquier aplicación pueda pasar a un entorno de producción.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

8.30 Desarrollo subcontratado[1]

La institución debe dirigir, supervisar y revisar las actividades relacionadas con el desarrollo de sistemas contratados.

Propósito

Garantizar que las medidas de seguridad de la información requeridas por la institución se implementen en el desarrollo de sistemas subcontratados.

Orientación

Cuando se contrata el desarrollo del sistema, la institución debe comunicar y acordar los requisitos y expectativas, y monitorear y revisar continuamente si la entrega del trabajo subcontratado cumple con las siguientes expectativas:

a) Se deben de establecer todos los requisitos contractuales con respecto a acuerdos de licenciamiento, propiedad intelectual, prácticas seguras de diseño, codificación y pruebas.

b) Se debe de generar todo un estudio de amenazas al utilizar un desarrollador externo.

c) Se deben de realizar todas las pruebas pertinentes de aceptación para la calidad y exactitud de los entregables; además de pruebas para establecer que se cumplen con los mínimos aceptables de seguridad en las aplicaciones, protección de contenido malicioso y protección contra las vulnerabilidades conocidas.

[1] *En el ICE el término usado es contratado en vez de subcontratado, se mantiene el subcontratado por cuestiones de homologación con la norma*.

d) Se deben de establecer los requisitos de seguridad para el entorno de desarrollo, incluyendo que se adapten a la postura de la institución en el ciclo de vida del desarrollo seguro.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

8.31 Separación de los entornos de desarrollo, prueba y producción

Los entornos de desarrollo, prueba y producción deben estar separados y asegurados.

Propósito

Proteger el entorno de producción y los datos contra el compromiso de las actividades de desarrollo y prueba.

Orientación

Debe identificarse e implementarse el nivel de separación entre los entornos de producción, prueba y desarrollo que es necesario para evitar problemas de producción.

a) Los entornos informáticos de producción deben estar lógica o físicamente separados de los entornos de desarrollo y prueba.
b) El acceso de los desarrolladores a los entornos de producción estará prohibido o limitado a la resolución de problemas y toda la actividad registrada y monitoreada.
c) Los procedimientos de inicio de sesión y las contraseñas serán diferentes para los entornos de producción y desarrollo/prueba.
d) Deberán existir procedimientos para transferir software o hardware desde el desarrollo y la prueba hasta la producción.
e) Cuando la separación física para el desarrollo/prueba no sea factible, las medidas de seguridad deberán ser iguales o superiores a las requeridas para el entorno de producción.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

8.32 Gestión del cambio

Los cambios en las instalaciones de procesamiento de la información y en los sistemas de información deben estar sujetos a los procedimientos de gestión del cambio.

Propósito

El propósito de este control de gestión de cambios del ICE es establecer las reglas para la creación, evaluación, implementación y seguimiento de los cambios realizados en los activos de Información.

Orientación

La introducción de nuevos sistemas y cambios importantes en los sistemas existentes debe seguir reglas acordadas y un proceso formal de documentación, especificación, prueba, control de calidad e implementación administrada. Deben existir responsabilidades y procedimientos de gestión para garantizar un control satisfactorio de todos los cambios.

Los procedimientos de control de cambios deben documentarse y aplicarse para garantizar la confidencialidad, integridad y disponibilidad de la información en las instalaciones de procesamiento de información y los sistemas de información, durante todo el ciclo de vida del desarrollo del sistema, desde las primeras etapas de diseño hasta todos los esfuerzos de mantenimiento posteriores.

El control de Gestión de Cambios del ICE se aplica a cualquier individuo, entidad o proceso que cree, evalúe y/o implemente cambios en los activos de Información. A continuación, se detallan las acciones que deben tener en cuenta para realizar cambios en los activos de información:

a) Los cambios en los activos de información de producción (empresa) deben documentarse y clasificarse de acuerdo con su:
    - Importancia

- Urgencia
- Impacto
- Complejidad

b) La documentación de cambios debe incluir, como mínimo:
   - Fecha de presentación y fecha de cambio,
   - Información de contacto del propietario y del custodio,
   - Naturaleza del cambio,
   - Solicitante de cambio,
   - Cambiar clasificación(es),
   - Plan de retroceso (Roll-Back)
   - Cambiar aprobador
   - Implementador de cambios
   - Indicación de éxito o fracaso

c) Los cambios con un impacto potencial significativo en los activos de información de la institución deben programarse.

d) Los responsables de activos de información deben ser notificados de los cambios que afectan a los sistemas de los que son responsables.

e) Se deben establecer ventanas de cambio autorizadas para cambios con un alto impacto potencial.

f) Los cambios con un impacto potencial significativo y/o una complejidad significativa deben tener pruebas de usabilidad, seguridad e impacto y planes de reversión incluidos en la documentación del cambio.

g) La documentación de control de cambios debe mantenerse de acuerdo con el Programa de Retención de Datos del ICE.

h) Los cambios realizados en los entornos y/o aplicaciones del cliente del ICE deben comunicarse a los clientes, de conformidad con los acuerdos y/o contratos vigentes.

i) Todos los cambios deben ser aprobados por el responsable del activo de información, previa aprobación del director, jefe de división o gerente, según sea el caso.

j) Los cambios de emergencia (es decir, ruptura/reparación, respuesta a incidentes, etc.) pueden implementarse de inmediato y completar el proceso de control de cambios de manera retroactiva.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.

8.33 Información de la prueba

La información de las pruebas debe seleccionarse, protegerse y gestionarse adecuadamente.

Propósito

Garantizar la pertinencia de las pruebas y la protección de la información operativa utilizada en éstas.

Orientación

La información de las pruebas debe seleccionarse para garantizar la fiabilidad de los resultados de las pruebas y la confidencialidad de la información operativa pertinente. La información sensible (incluida la información de identificación personal) no debe copiarse en los entornos de desarrollo y pruebas.

Los siguientes puntos deben aplicarse para proteger las copias de la información operativa, cuando se utilicen con fines de prueba, tanto si el entorno de prueba se construye internamente como en un servicio en la nube:

a) El manejo de la información de prueba debe estar autorizados siempre y cuando se cumpla con los acuerdos de confidencialidad, integridad y disponibilidad, además, que exista un contrato de servicio y el proveedor cumpla con los requerimientos de las normas y legislaciones vigentes.
b) Aplicar a los entornos de prueba los mismos procedimientos de control de acceso que se aplican a los entornos operativos;
c) Tener una autorización separada cada vez que se copie la información operativa a un entorno de prueba;
d) En los casos que exista un contrato con terceros para mantenimientos preventivos o correctivos, se hará mención expresa dentro de las cláusulas de éste, sobre el

deber de confidencialidad del proveedor en relación con la información involucrada en los servicios prestados y a la que accede para brindar éstos.

e) Registrar la copia y el uso de la información operativa para proporcionar una pista de auditoría;

f) La información de las pruebas debe almacenarse de forma segura (para evitar su manipulación, que de otro modo podría dar lugar a resultados no válidos) y utilizarse únicamente con fines de prueba.

g) Las pruebas de sistemas y de aceptación pueden requerir volúmenes considerables de información de prueba que se acerquen lo más posible a la información operativa.

h) Proteger la información sensible mediante la eliminación o el enmascaramiento si se utiliza para las pruebas.

i) Eliminar adecuadamente la información operativa de un entorno de pruebas inmediatamente después de que éstas hayan finalizado para evitar el uso no autorizado de la información de las pruebas.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
19.00.004.2005	Procedimiento para las Auditorías de los Sistemas de Gestión.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.
19.00.001.2017	Lineamientos para el Funcionamiento del Modelo de Arquitectura de Información Empresarial para el Grupo ICE.

8.34 Protección de los sistemas de información durante las pruebas de auditoría

Las pruebas de auditoría y otras actividades de garantía que impliquen la evaluación de los sistemas operativos deben planificarse y acordarse entre el encargado de las pruebas y la dirección correspondiente.

Propósito

Minimizar el impacto de las auditorías y otras actividades de aseguramiento en los sistemas operativos y los procesos de negocio.

Orientación

Coordinar la auditoría con el titular subordinado respectivo el acceso a los sistemas y datos de acuerdo con los siguientes pasos:

a) Acordar y controlar el alcance de las pruebas de auditoría técnica.

b) Limitar las pruebas de auditoría al acceso de sólo lectura al software y a los datos. Si no se dispone de acceso de sólo lectura para obtener la información necesaria, ejecutar la prueba por un administrador experimentado que tenga los derechos de acceso necesarios en nombre del auditor.

c) Si se concede el acceso, establecer y verificar los requisitos de seguridad establecidos por parte del personal del CSIRT para garantizar que cumplan como mínimo con antivirus, versiones licenciadas de los programas y sus respectivos parches de los dispositivos utilizados para acceder a los sistemas antes de permitir el acceso.

d) Sólo permitir el acceso a copias aisladas de los archivos del sistema que no sean de sólo lectura, borrándolas cuando la auditoría haya terminado, o dándoles la protección adecuada si existe la obligación de conservar dichos archivos en virtud de los requisitos de la documentación de auditoría.

e) Identificar y acordar las solicitudes de tratamiento especial o adicional, como la ejecución de herramientas de auditoría.

f) La realización de pruebas de auditoría que puedan afectar a la disponibilidad del sistema fuera del horario laboral; la supervisión y el registro de todos los accesos con fines de auditoría y prueba.

g) Las pruebas de auditoría y otras actividades de aseguramiento también pueden tener lugar en los sistemas de desarrollo y de prueba, donde éstas pueden afectar, por ejemplo, a la integridad del código o llevar a la divulgación de cualquier información sensible que se encuentre en dichos entornos.

h) La verificación de controles en el procesamiento de la información e instalación de sistemas, con el objetivo de evaluar su efectividad y presentar también alguna recomendación y consejo.

i) Verificar y juzgar de manera objetiva la información.

j) Examen y evaluación de los procesos en cuanto a informatización y trato de datos se refiere. Además, se evalúa la cantidad de recursos invertidos, la rentabilidad de cada proceso y su eficacia y eficiencia.

Documentos Relacionados

Código	Ley, Política, Norma
89.00.001.2023	Política Corporativa de Ciberseguridad.
38.04.001.2008	Política Empresarial de Seguridad de la Información.
38.00.002.2013	Política Corporativa de Confidencialidad de la Información.
10.00.003.2009	Política Empresarial de Protección y Seguridad Física y Lógica.
19.00.004.2005	Procedimiento para las Auditorías de los Sistemas de Gestión.
36.00.001.2009	Reglamento para Utilización de Recursos Informáticos de Usuario Final: Hardware, Software y Servicio de Comunicaciones.
19.00.001.2017	Lineamientos para el Funcionamiento del Modelo de Arquitectura de Información Empresarial para el Grupo ICE.

9 VIGENCIA DEL DOCUMENTO

Este documento rige a partir de su publicación.

10 REVISIÓN Y ACTUALIZACIÓN

La Dirección Ciberseguridad de la Gerencia Tecnología y Soluciones Digitales, coordinará la revisión y actualización del presente documento, con una periodicidad anual y planteará las modificaciones que estime pertinentes.

11 DEROGATORIA

Este documento deroga los Lineamientos de Seguridad de la Información, 38.00.002.2016 MC, versión 2.

12 CONTROL DE CAMBIOS

No aplica

13 CONTROL DE ELABORACIÓN, REVISIÓN Y APROBACIÓN

ELABORÓ	DEPENDENCIA	FECHA
Edith Guevara Espinoza	Dirección Ciberseguridad	24/05/2022
María Laura Quesada Martínez	Dirección Ciberseguridad	
Karen Córdoba Peraza	Dirección Ciberseguridad	
Víctor Villalobos Oviedo	Dirección Ciberseguridad	
Luis Fernando Bonilla Zúñiga	Dirección Ciberseguridad	
Pablo López Aguilar	Dirección Ciberseguridad	
Eric Solórzano Jiménez	Dirección Ciberseguridad	
Mike Zamora González	Dirección Ciberseguridad	
Roy Hidalgo Madrigal	Dirección Ciberseguridad	
Michael Hernández Alvarado	Dirección Ciberseguridad	
Ledia Morales Lara	Dirección Ciberseguridad	

REVISÓ	FIRMA
Sra. Vera Bonilla Solís. Gerencia Tecnología y Soluciones Digitales	VERA INES BONILLA SOLIS (FIRMA) Firmado Digitalmente Fecha: 15/11/2023 18:19:47 CST Localización: Costa Rica
Sr. Melvin Monge Sandí. Gerencia Servicios y Recursos Empresariales	MELVIN EDUARDO MONGE SANDI (FIRMA) Firmado Digitalmente Fecha: 21/12/2023 14:50:25 CST Localización: Costa Rica
Sr. Roberto Quirós Balma. Gerencia de Electricidad	ROBERTO MIGUEL QUIROS BALMA (FIRMA) Firmado Digitalmente Fecha: 21/12/2023 16:11:24 CST Localización: Costa Rica

REVISÓ	FIRMA
Sr. Keiner Arce Guerrero. Gerencia Finanzas	KEINER ARCE GUERRERO (FIRMA) Firmado Digitalmente Fecha: 17/01/2024 15:42:16 CST Localización: Costa Rica
Sr. Luis Diego Abarca Fernández. Gerencia Telecomunicaciones	LUIS DIEGO ABARCA FERNANDEZ (FIRMA) Firmado Digitalmente Fecha: 17/01/2024 15:51:19 CST Localización: Costa Rica

APROBÓ	FIRMA
Sr. Harold Cordero Villalobos Gerencia General	HAROLD CORDERO VILLALOBOS (FIRMA) Firmado digitalmente por HAROLD CORDERO VILLALOBOS (FIRMA) Fecha: 2024.01.23 15:25:03 -06'00'