POLÍTICAS INSTITUCIONALES

POLÍTICA DE SEGURIDAD INFORMÁTICA

Comfamiliar RISARALDA

Introducción

Con el propósito de ayudar a preservar los activos de información (hardware, software, datos e información generada) que hacen parte del funcionamiento y son la base de crecimiento de la Institución, se fundamenta en instrucciones básicas una Política para garantizar el rendimiento y continuidad de la dinámica laboral y que hará parte del reglamento interno de trabajo de la organización.

Se define esta Política como un documento de directrices preventivas, que ilustran textualmente los diversos caminos para evitar ataques y disminuir riesgos a través de un conjunto de elementos estratégicos, procedimientos, códigos de conducta, normas y directrices organizacionales, con el fin de asegurar la vida practica tanto del personal de trabajo como la vida útil de los recursos informáticos.

Alcance

La Política de Seguridad Informática está orientada a establecer medidas para proteger las tecnologías informáticas (equipos de cómputo, sistemas de información, redes), necesarias para asegurar la confidencialidad, integridad, confiablidad y disponibilidad de la información. Aplica a todas las áreas de la entidad desde la recolección del dato hasta su transformación en información para la toma de decisiones.

Declaración de Compromiso

Comfamiliar Risaralda adquiere el compromiso de velar por la implementación y cumplimiento de la Política Informática, de aplicar dichas políticas y de darla a conocer a sus empleados y a los terceros. Además adquiere el compromiso de salvaguardar toda información generada, procesada, utilizada en los sistemas de información, implementando medidas preventivas para proteger las tecnologías informáticas evitando ataques y mitigando riesgos.

Marco de Actuación

1. SEGURIDAD FRENTE AL ACCESO POR PARTE DE TERCEROS

El acceso de terceros debe ser controlado por requerimientos de seguridad y compromisos de confidencialidad, y es responsabilidad de cada proceso o servicio de la entidad.

2. CONTROL DE ACTIVOS DE INFORMACIÓN

2.1. Activos tangibles/bienes físicos
Todo recurso informático perteneciente a la organización, deberá ser inventariado y plaqueteado. El uso que se da a los equipos cuando son retirados de la Institución es responsabilidad del usuario y está sujeto a los términos del contrato. Toda reubicación de los equipos deberá notificarse al Proceso de Sistemas. Ningún equipo deberá ser abierto o manipulado por los colaboradores ni tratar de ser reparados por personal no autorizado. Cuando un recurso informático de la organización se extravía o es hurtado, deberá informarse inmediatamente al Jefe de Servicios Generales y tramitar la denuncia ante las autoridades competentes.

2.2. Activos intangibles/bienes lógicos (datos procesados / información)
El Proceso de Sistemas es el responsable de realizar las copias de seguridad de los servidores, tal y como se describe en el procedimiento Realización y Administración de Copias de Seguridad. Las copias de seguridad de los equipos de cómputo son responsabilidad del usuario. Todo software producido y adquirido por la organización estará debidamente inventariado. Ningún funcionario podrá instalar software sin la debida autorización. El contenido lógico de los equipos de cómputo deberá ser de carácter corporativo, por lo que se prohíbe tener archivos personales.

3. CONTROL DE ACCESOS

3.1. Identificación, autenticación y control de acceso a sistemas de información
La creación, modificación, o inactivación de usuarios deberán ser gestionadas a través del Módulo de Soporte, de acuerdo con lo definido en el procedimiento Administración y control de accesos a servicios de TI. El proceso de Sistemas deberá hacer revisiones periódicas eliminando usuarios en estado inactivo por más de 90 días. El uso de herramientas de soporte para acceso remoto solo está autorizado para el personal de soporte técnico con previa aprobación de la conexión.

3.2. Acceso a las instalaciones (procesos críticos: data center)
El personal autorizado para ingresar a los DataCenter, solo podrá hacerlo mediante el uso del sistema de control de acceso basado en la lectura de tarjetas de proximidad y clave. Además, se controlaran las entradas en horarios previamente establecidos, si en algún momento se requiere la entrada en horario no laboral, deberá ser autorizado por el Líder de Tecnología Informática.

3.3. Infraestructura de redes y telecomunicaciones
El Proceso de Sistemas deberá llevar el inventario total de la infraestructura disponible.

3.4. Navegación en internet
El acceso a la red de internet es responsabilidad de cada usuario y no deberá dejar que otra persona obtenga acceso a través de su cuenta.

3.5. Intranet y correo electrónico corporativo
Los mensajes corporativos de carácter informativo serán visualizados en la página principal de SEC, http://sec.comfamiliar.com y serán responsabilidad del proceso de Mercadeo y Relacionamiento Estratégico. El correo electrónico corporativo y la mensajería interna, son de uso exclusivamente laboral y como tal, susceptible de ser monitoreados y/o auditados en relación con los mensajes enviados y recibidos, así como los documentos adjuntos a los mismos. El correo corporativo no debe ser utilizado para el envío de cadenas. La responsabilidad del backup de las cuentas de correo es responsabilidad del usuario.

4. CONFIDENCIALIDAD DE LA INFORMACIÓN
Toda persona contratada por la organización, deberá firmar como parte del contrato la cláusula de confidencialidad de la información. Se debe firmar acuerdos de confidencialidad y de nivel de servicio con proveedores que tengan relación directa con información crítica de la organización.

5. HERRAMIENTAS DE SEGURIDAD – ANTIVIRUS – CONTROL DE INVENTARIOS
Todos los equipos de cómputo de la entidad que tengan sistema operativo Windows deberán tener instalado, actualizado y en ejecución el software antivirus y el software de control de inventarios corporativos, como medida de prevención para ataques externos e internos.

Normatividad Aplicable

- Ley 23 de 28 de enero de 1982 “Sobre Derechos de Autor”
- Ley 44 de 1993 “Por la cual se modifica y adiciona la ley 23 de 1982”
- Ley 1273 de 5 de Enero de 2009 “Protección de la información y de los datos” Ley 527 de 1999; Mensaje de Datos, Comercio Electrónico y Firmas Digitales
- Ley 565 de 2 de febrero de 2000. “Tratado de la OMPI – sobre Derechos de Autor”; Ley 603 de 2000; “Propiedad Intelectual y Derechos de Autor”
- Ley 1273 de 2009 “Delitos informática”

Responsables de Gestión

LÍDER DE TECNOLOGÍA INFORMÁTICA, persona dotada de conocimiento técnico, encargada de velar por

la seguridad de la información y de llevar un estricto control con la ayuda de la unidad de informática referente a los servicios prestados y niveles de seguridad aceptados para tales servicios.

UNIDAD DE SISTEMAS, entidad o departamento dentro de la organización, que vela por todo lo relacionado con la utilización de computadoras, sistemas de información, redes informáticas, procesamiento de datos e información y la comunicación en sí, a través de medios electrónicos.

Documentos Relacionados

- 1-PR-139 Realización y Administración de Copias de Seguridad
- 1-PR-108 Administración y Control de Accesos a Servicios de TI
- 1-PR-090 Soporte Técnico

Conceptos (Glosario)

ACTIVO INTANGIBLE: Activos que no tienen soporte físico, ya que están basados, principalmente, en la información y el conocimiento, por lo que su identificación y cuantificación se hace difícil, como patentes, marcas, software informático o sistema de información, bases de datos.

ACTIVO TANGIBLE: Activos de la empresa que tienen un soporte físico y se concretan en algo material, por lo que pueden ser fácilmente identificados y cuantificados en el seno empresarial, como computadores, portátiles, servidores, impresoras, escáneres, proyectores, entre otros.

ANTIVIRUS: Programa para prevenir, detectar y eliminar virus informáticos, Worms, troyanos y otros invasores indeseados que puedan infectar su ordenador. Principales daños: pérdida de rendimiento del procesador, borrado de archivos, alteración de datos, información confidencial expuesta.

ATAQUE: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema de información.

AUTENTICACIÓN: Confirmación que se realiza a través de los medios electrónicos de la identidad de un individuo o de un organismo, así como de todas sus operaciones, transacciones y documentos.

DATO: Representación simbólica, números o letras de una recopilación de información, puede ser cualitativa o cuantitativa, que facilitan la deducción de un hecho. Un dato no tiene valor semántico en sí mismo, pero al ser procesado puede servir para realizar cálculos o tomar decisiones.

DISPONIBILIDAD: Los recursos de información sean accesibles, cuando estos sean necesarios.

INFORMACIÓN: Conjunto de datos, añadidos, procesados y relacionados, de manera que pueden dar pauta a la correcta toma de decisiones según el fin previsto.

INTEGRIDAD: Proteger la información de alteraciones no autorizadas por la organización.

INTRANET: Red informática interna de una empresa u organismo, basada en los estándares de Internet, en la que las computadoras están conectadas a uno o varios servidores web.

RIESGO: Posibilidad de que se produzca un impacto en un activo, dominio o en la organización.

SERVIDOR: Es un ordenador o maquina informática que está al "servicio" de otras máquinas, ordenadores o personas llamadas clientes y que le suministran a estos, todo tipo de información.