

INFORMACION GENERAL DEL DOCUMENTO

OBJETIVO

Establecer las actividades que permitan garantizar la protección de los bienes informáticos y la seguridad de la información.

ALCANCE

Aplica a todos los colaboradores que requieran procesar información de la organización para el desarrollo de sus actividades laborales.

RESPONSABLES

Facilitador Junior de Tecnología
Auxiliar de Tecnología
Colaboradores

RECURSOS

Humano: personal del proceso de tecnología y administrativos
Tecnológicos: Sistemas de Información de la organización, Circuito Cerrado de Televisión.

INDICADOR

NOMBRE: Realización de Back up
INDICE: No. de *Back up* realizados
FRECUENCIA: Mensual
RESPONSABLE: Auxiliar de Tecnología

META

Cumplir con el **100%** de los back up

PERIODICIDAD DE REVISIÓN Y EVALUACION

Fecha de inicio: 17 de Enero de 2014
Vigencia: 1 año
Revisión Anual
Evaluación: Anual
Nota: el programa podrá ser modificado al presentarse cambios en las actividades desarrolladas, se realizará seguimiento por medio del registro y análisis de indicadores.

DOCUMENTOS RELACIONADOS

ELABORÓ Rubén Darío Herrera Gómez Facilitador Junior de Tecnología		REVISÓ Carlos Fernando Rodríguez Facilitador Jr. De Seguridad		APROBÓ Carmen Lucía Rodríguez Dinamizadora Ejecutiva	
FIRMA	FECHA	FIRMA	FECHA	FIRMA	FECHA

GH D 01 F 08 Paz y Salvo
 GA I 01 Instructivo para *back up*
 GA I 01 F 01 Entrega copias de seguridad
 SG PL 01 Plan de emergencias
 Informes de auditoría externa
 Contratos de Trabajo
 Acuerdos de confidencialidad
 Back up de la información

REQUISITOS LEGALES APLICABLES

Ley 1273 de 2010 Delitos Informáticos. Artículo 269 literal a, b, c, d, e, f, g.

ASPECTOS GENERALES

Para Timón S.A. es un propósito fundamental el proteger los recursos informáticos y tecnológicos empleados en el desarrollo de sus actividades, previniendo la materialización de riesgos internos o externos, deliberados o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

- Se considera un situación de emergencia en seguridad la ocurrencia de una situación que indica una posible violación a la seguridad de la información o fallas en los controles que genere un impacto en el desarrollo de las operaciones de la organización y que puede ser controlado rápidamente.
- Todos los colaboradores de la organización deben reportar cualquier situación que pueda comprometer la preservación de la confidencialidad, disponibilidad y/o integridad de la información.
- La alta gerencia o quien este delegue son los únicos autorizados para comunicar situaciones que comprometan la seguridad de la información ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.
- Las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.
- Se considera información crítica, aquella referente a los sistemas de información que maneja la organización, los correos electrónicos, las grabaciones del Circuito Cerrado de Televisión (CCTV), y la información del sistema integrado de gestión y la manejada por el proceso de Gestión Financiera.
- Los equipos que hacen parte de la infraestructura tecnológica de la organización como servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, plantas telefónicas, son ubicados en lugares seguros protegidos contra amenazas o peligros del entorno.
- Ninguno de los usuarios está autorizado para extraer o cambiar *hardware* de los equipos de la organización, ni realizar traslados, sin previa autorización del proceso de Tecnología. Así mismo, no están autorizados para descargar vía Internet o instalar programas ajenos a la organización y sin la licencia correspondiente.


DESCRIPCION DE ACTIVIDADES A DESARROLLAR

ACTIVIDAD	RESPONSABLE	PERIODO DE VIGENCIA Y/O FRECUENCIA	REGISTRO
<p>ACUERDOS DE CONFIDENCIALIDAD DE LA INFORMACIÓN</p> <p>Todos los colaboradores y/o terceros deben aceptar los acuerdos de confidencialidad definidos por la organización, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.</p> <p>Para el caso de contratistas, los respectivos contratos y/u órdenes de prestación de servicios deben incluir un acuerdo de confidencialidad.</p> <p>Todos los colaboradores deben firmar el acuerdo de confidencialidad durante el proceso de contratación previo inicio de sus actividades laborales.</p> <p>El proceso de Gestión Humana es el encargado del proceso de terminación o cambio de contratación de los colaboradores de la organización, en tal sentido una vez informada de la terminación o cambio de contratación, se le entrega al colaborador el formato GH D 01 F 08 Paz y salvo.</p> <p>Para firmar el Paz y salvo por parte del Facilitador Jr. de Tecnología, se debe realizar la desactivación de los usuarios de red asignados al colaborador, así como la revisión de los medios tecnológicos asignados y realizar la copia de seguridad e la información que tenga a su cargo. Es importante de que los medios tecnológicos que fueron asignados al colaborador sean regresados en buen estado.</p>	<p>Analista de selección y contratación Gestión Humana</p> <p>Analista de Tecnología</p> <p>Facilitador Jr. de Tecnología</p>	<p>Año 2014 / Permanente</p>	<p>Contratos de Trabajo Acuerdos de confidencialidad</p> <p>Back up de la información</p> <p>GH D 01 F 08 Paz y Salvo</p>
<p>ASIGNACIÓN DE ACTIVOS TECNOLÓGICOS</p> <p>Para el control de activos tecnológicos como equipos, hardware y software, se controlan a través del inventario de activos, donde se lleva un registro de la asignación de equipos de cómputo por colaborador, las características y ubicación de equipos comunes como (impresoras, escáneres, servidores, equipos activos, entre otros).</p> <p>Mensualmente, se realiza la verificación del uso dado del <i>hardware</i>, <i>software</i>, y los archivos a los cuales accede el</p>	<p>Facilitador Jr. de Tecnología</p> <p>Analista de Tecnología</p>	<p>Año 2014 / control de asignación permanente</p>	<p>Comunicado interno de asignación de equipos</p> <p>Informe de inspección periódica de equipos de cómputo</p>

<p>colaborador, teniendo en cuenta que los equipos de cómputo de los colaboradores no tienen activo el permiso de borrar el historial de búsqueda, lo que facilita la trazabilidad y verificación de las páginas visitadas.</p> <p>De este ejercicio se genera Informe de inspección periódica de equipos de cómputo.</p>		Control de uso a equipos asignados Mensual.	
<p>REALIZACION DE BACK UP</p> <p>Para la protección de información en medios magnéticos, mensualmente se realiza back up a los computadores de los colaboradores y se almacena en un servidor ubicado en las instalaciones del Taller de Timón. A los colaboradores administrativos de los procesos de operaciones y mantenimiento en Timón Bogotá se les realiza <i>back up</i> según Instructivo para <i>Back up</i>.</p> <p>Una vez realizado el <i>back up</i> a la información, el personal de tecnología salvaguarda la información en un disco duro extraíble y se entrega al proceso de seguridad que se encuentra en una sede diferente como una medida de contingencia en el caso de presentarse una situación de emergencia relacionada con la pérdida de información de la organización.</p> <p>El proveedor OET genera replica de información, sincronización diaria que se realiza entre la 1:10 y 3:00 p.m.</p> <p>El circuito cerrado de televisión se le realiza Back up mensualmente, el cual es almacenado por un mes. En caso de presentarse alguna novedad, se conservara la información relacionada en forma parcial.</p>	<p>Auxiliar de Tecnología</p> <p>Facilitador Jr. de Tecnología</p> <p>Facilitador Jr. de Seguridad</p>	<p>Año 2014 / Mensualmente</p>	<p>GA I 01 Instructivo para <i>back up</i></p> <p>GA I 01 F 01 Entrega copias de seguridad</p> <p>SG PL 01 Plan de emergencias</p> <p>Disco con almacenamiento de copia de seguridad mensual.</p>
<p>PROTECCION DE SOFTWARE</p> <p>Los equipos de cómputo cuentan con el bloqueo para no permitir la instalación o desinstalación de <i>software</i>, y en caso de ser necesaria la instalación o desinstalación de algún <i>software</i> se realiza la solicitud al proceso de Tecnología por medio del aplicativo SIANT (Sistema Integrado de Administración de Novedades Timón) y se ejecuta su tratamiento.</p> <p>Adicionalmente los medios tecnológicos cuentan con controles que detectan y previenen códigos maliciosos: Corta fuegos, antivirus, <i>anti spam</i> y <i>antimalware</i>.</p>	Facilitador Jr. de Tecnología	Año 2014 / Permanente en equipos	Permanentemente

BLOQUEO DE PUERTOS USB Se realiza el bloqueo de puertos USB a los computadores con el propósito de evitar la fuga de información por medio de USB no autorizadas por la organización. Este bloqueo se realiza permanentemente a los equipos, y se dejan ciertos equipos sin este bloqueo ya que necesitan algún tipo de extracción de información. Es importante aclarar que los equipos sin este control están a cargo de Líderes de proceso	Auxiliar de Tecnología	Año 2014 / permanente	Permanentemente
SIMULACROS Se realizarán simulacros para preparar y concientizar a todos los colaboradores de la organización a adoptar las rutinas de acción y planes establecidos para afrontar una situación de emergencia.	Facilitador Jr. de Tecnología	Año 2014 / Semestralmente	SG I 05 F 01 Registro de Simulacros
2.1 SEGUIMIENTO Y CONTROL			
REGISTRO DE CUMPLIMIENTO (criterio operacional)	PERIODICIDAD TOMA DE DATOS	PERIODO DE VIGENCIA Y/O FRECUENCIA	RESPONSABLE
Back up de la información GA I 01 F 01 Entrega copias de seguridad SG I 05 F 01 Registro de Simulacros	De acuerdo al desarrollo de las actividades	Año 2014	Facilitador Jr. de Tecnología
2.2..TIPO DE MEDIDA DE INTERVENCIÓN			
CONTROL	X	MITIGACIÓN	X
PREVENCIÓN	X		

3.CONTROL DE CAMBIOS		
Versión	Modificación	Fecha
1	Elaboración del programa.	17/Ene/2013
2	Se define la frecuencia en la que se realiza la verificación del uso del <i>hardware</i> y <i>software</i> de los equipos por parte de los colaboradores y se define como registro de dicha actividad el informe de inspección periódica a equipos de cómputo.	18/Abr/2013
3	Se le incluyo columna de periodo y vigencia/frecuencia, se actualizo el cargo del líder de seguridad y Tecnología. Se revisaron y actualizaron las actividades asociadas al programa, incluyendo la actividad simulacros. Se modifica la frecuencia de la revisión a anual. Se incluye en la actividad realización de Back up lo relacionado con CCTV	13/Mar/2014

	PROGRAMA PARA LA SEGURIDAD DE LA INFORMACION	CÓDIGO:	SG D 01 PR 02
		VERSIÓN:	4
		Página 6 de 6	

3.CONTROL DE CAMBIOS		
Versión	Modificación	Fecha
4	Se realiza revisión general del programa con los colaboradores responsables y actualización de funcionarios responsables de actividades.	10/Mar/2015

COPIA NO CONTROLADA