

	POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Clasificación: 2
		Versión: 6.0
		Fecha de Actualización: 29/02/2024

ÍNDICE

1. Contenido.
 - 1.1. Objetivo general.
 - 1.2. Objetivos específicos.
 - 1.3. Infraestructura general del proceso.
2. Seguridad de la información.
 - 2.1. Seguridad de la información ¿Qué es?
 - 2.2. Seguridad de red.
 - 2.3. Seguridad física.
 - 2.4. Seguridad de los datos.
 - 2.5. Backup de la información.
 - 2.6. Backup Hardware.
 - 2.7. Hacking etico
3. Política de usuarios, contraseñas, utilización de la información y visitas.
 - 3.1. Por fuera de la compañía.
 - 3.2. Al interior de la compañía.
 - 3.3. Personal Visitante.
 - 3.4. Clasificación de la información corporativa.
 - 3.5. Cifrado de la información.
4. Incidencias.
 - 4.1. Reporte de incidencias.
5. Auditorías internas y de calidad para la seguridad de la información.
6. Plan de continuidad del negocio.
 - 6.1. Plan de BCP.
 - 6.2. Roles BCP, organización de los equipos.
 - 6.3. Workflow del BCP.
 - 6.4. Excepciones.

Elaborado por: Director administrativo y director de T. I	Revisado por: Director administrativo y auditor interno	Aprobado por: presidente
Fecha: 29/02/2024	Fecha: 29/02/2024	Fecha: 29/02/2024

	POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Clasificación: 2
		Versión: 6.0
		Fecha de Actualización: 29/02/2024

1. CONTENIDO
<p>El presente documento se realiza con el fin de robustecer el proceso de seguridad de la información a fin de asegurar que la prestación de los diferentes servicios que RST Asociados S.A.S les brinda a sus diferentes clientes se realice con seguridad, calidad y confiabilidad.</p> <p>También se crea para elevar los estándares de calidad corporativa ya que según la misión y la visión empresarial, estos procesos deben asegurar y garantizar la satisfacción entera de los clientes de RST Asociados S.A.S.</p>
1.1. OBJETIVO GENERAL
<p>El presente documento se realiza con el fin de robustecer el proceso de seguridad de la información a fin de asegurar que la prestación de los diferentes servicios que RST Asociados S.A.S les brinda a sus diferentes clientes se realice con seguridad, calidad y confiabilidad.</p> <p>También se crea para elevar los estándares de calidad corporativa ya que según la misión y la visión empresarial, estos procesos deben asegurar y garantizar la satisfacción entera de los clientes de RST Asociados S.A.S.</p>
1.2. OBJETIVO ESPECÍFICOS
<ul style="list-style-type: none">• Crecer de la mano con nuestros clientes para estar al servicio cada una de las unidades de negocio con los estándares más solicitados dentro del mercado.• Generar una política de seguridad sólida para cubrir las necesidades de los clientes.• Proteger el activo más importante de la compañía (información).• Evolucionar con los requerimientos que día a día nuestros clientes más exigentes solicitan para la operación de sus cuentas y servicios.
1.3. INFRAESTRUCTURA GENERAL DEL PROCESO
<p>Las labores del personal de RST Asociados S.A.S están apoyadas por herramientas de Contact Center, en lo relacionada con la parte de consecución de información salarial, realizando llamadas, confirmando información y en la parte de la administración, custodia y seguridad de la información a más de los aplicativos y software propiedad de RST Asociados S.A.S.</p>

Elaborado por: Director administrativo y director de T. I	Revisado por: Director administrativo y auditor interno	Aprobado por: presidente
Fecha: 29/02/2024	Fecha: 29/02/2024	Fecha: 29/02/2024

	POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Clasificación: 2
		Versión: 6.0
		Fecha de Actualización: 29/02/2024

2. SEGURIDAD DE LA INFORMACIÓN
2.1. SEGURIDAD DE LA INFORMACIÓN ¿QUÉ ES?
<p>Se determina que la seguridad de la información para RST Asociados, son el conjunto de actividades que se ejecutan, con el fin de asegurar que la información esté disponible cuando sea necesaria y que la misma cuente con sus respectivas copias de seguridad (Backup) a fin de restaurar información vital de la compañía tanto del hardware como del software.</p> <p>La seguridad de la información para RST Asociados está compuesta de diferentes protocolos que se aseguran de que la información se encuentre protegida los cuales son:</p> <ul style="list-style-type: none"> • Seguridad de red. • Seguridad física. • Seguridad de los datos. • Backup de la información. • Backup de los dispositivos hardware. <p>Se designa al Director de TI como representante de RST ante los clientes y demás partes interesadas como oficial o líder de cumplimiento en el Sistema de Gestión de Seguridad de la Información.</p> <p>Es responsabilidad del Director de TI el reportar a Presidencia, entes de control o clientes cuando aplique la ocurrencia de incidentes o eventos que afecten en la seguridad de la información para determinar e implementar los planes de acción acorde con la naturaleza del evento.</p> <p>Es responsabilidad del Director de TI en conjunto con el Director del SGC realizar la revisión y actualización de las políticas de seguridad de la información con Presidencia para determinar la necesidad de cambios o confirmación en su vigencia; esta revisión se debe hacer por lo menos con una frecuencia anual, o cuando sea necesario por parte de los clientes, o como resultado de las auditorías internas o externas.</p>
2.2. SEGURIDAD DE RED

Elaborado por: Director administrativo y director de T. I	Revisado por: Director administrativo y auditor interno	Aprobado por: presidente
Fecha: 29/02/2024	Fecha: 29/02/2024	Fecha: 29/02/2024



POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Clasificación: 2

Versión: 6.0

Fecha de Actualización:
29/02/2024

Todos los días, de la mano con la evolución tecnológica vienen las amenazas que ponen en peligro la información de las compañías, por lo que **RST Asociados S.A.S**, cuenta con un esquema de seguridad IT de red con un dispositivo de la empresa Fortinet, el cual es un firewall Fortigate 100E y un espejo de contingencia Fortigate 80c, los cuales todos los días se actualiza según los nuevos desarrollos de su empresa fabricante la cual cumple con los más altos estándares de calidad en relación con seguridad de la información relacionada a las redes de comunicaciones y datos de las compañías; en el caso puntual de **RST Asociados S.A.S** este firewall cuenta con las siguientes fortalezas.

1. **FIREWALL:** Es un sistema de seguridad de red, basado en aplicación de reglas programadas para permitir o bloquear los accesos a diferentes redes.
2. **ROUTER:** Al contar con distintos puertos internal y wan, este dispositivo está en la capacidad de realizar capa 3 y certificar en tiempo real que los datos que pasan entre cada LAN, Vlan y canal Wan, se encuentren correctamente certificadas como flujo de información segura ya que cada paquete de datos es analizado.
3. **POLICY NETWORK:** Interfaz que permite crear, modificar o eliminar permisos o bloqueos en la red.
4. **FIREWALL OBJETS Y VIRTUAL IP:** Sistema de creación de objetos (Direcciones IP) IP's virtuales para publicar en una wan y asignación de velocidad de navegación hacia internet y a la red misma para balancear las cargas de tráfico a través de los switches.
5. **SISTEMA UTM:** Este es un sistema avanzado para el tratamiento de amenazas de red con las cuales aumentó los esquemas de seguridad para los usuarios de la red, servidores y servicios publicados en internet; estas herramientas son:
 - **ANTIVIRUS:** Revisa conexiones FTP, pop, imap, http, HTTP, IM (Chat).
 - **FILTRADO WEB:** Crea políticas de navegación, según blacklist programables y categorización inteligente.
 - **APC CONTROL DE APLICACIONES:** Complementa el filtrado web bloqueando en la LAN o de los canales wan servicios como; Bootnet, IM, almacenamiento cloud, redes sociales, multimedia, proxy, email, accesos remotos, P2P, descargas y otras más.
 - **PROTECCIÓN CONTRA INTRUSOS:** Sensores especializados que detectan ataques en la red, DDoS, Inyecciones a bases de datos y demás, bloqueando de forma automática la conexión atacante.
 - **EMAIL FILTER:** Filtrado de puertos pop, imap, smtp y tráfico de correos electrónicos basados en la web donde se identifica el phishing y los spam con contenido peligroso para bloquearlos.
 - **DATA LEAK PREVENTION:** Sensor inteligente que ayuda con las correctas políticas a eliminar el riesgo de fraude y pérdida de información.
 - **VoIP:** Filtrado constante de la voz sobre IP bloqueando ataques a estos sistemas y previniendo el Bypass.
6. **SISTEMA VPN:** Sistema de conexiones privadas para conectar puntos fuera de la compañía a la oficina por un canal seguro, filtrado y encriptado.

Elaborado por: Director
administrativo y director de T. I

Fecha: 29/02/2024

Revisado por: Director administrativo
y auditor interno

Fecha: 29/02/2024

Aprobado por: presidente

Fecha: 29/02/2024



POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Clasificación: 2

Versión: 6.0

Fecha de Actualización:
29/02/2024

7. COMPLEMENTOS LDAP o AD: Permite brindar autenticación de usuarios para navegación, antivirus, recursos de red y demás por directorio activo o LDAP y ofrece la posibilidad de autenticar por token.

8. ENDPOINT PROTECTION: Herramienta para proteger a los clientes de la compañía dentro y fuera de ella y además realizar labores de antivirus y filtrado web.

El conjunto de estas herramientas hace que, con la administración necesaria, RST Asociados se encuentre protegida de amenazas de la red.

Elaborado por: Director
administrativo y director de T. I

Fecha: 29/02/2024

Revisado por: Director administrativo
y auditor interno

Fecha: 29/02/2024

Aprobado por: presidente

Fecha: 29/02/2024

	POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Clasificación: 2
		Versión: 6.0
		Fecha de Actualización: 29/02/2024

2.3. PROCESO DE SEGURIDAD DE LA RED

- 1. CREACIÓN DE VLAN Y DMZ:** Actualmente para ayudar a los switches y al firewall para gestionar mejor los recursos, hay creadas 6 Vlan y una DMZ distribuidas de la siguiente manera:
 - **VLAN_ADMINISTRA:** Pertenecen a contabilidad, tesorería, recursos humanos, gerencia administrativa, Departamento de TI, Analítica y presidencia.
 - **VLAN_BANCO_AGRARIO:** Exclusiva para la operación de Contact Center.
 - **VLAN BIOMÉTRICO:** Exclusiva para el área de sistemas.
 - **VLAN_SERVIDORES:** Exclusiva para los servidores.
 - **DMZ:** Dedicada para el departamento Jurídico.
- 2. POLÍTICAS DE NAVEGACIÓN:** La navegación está sujeta a la autorización expresa de la gerencia donde cada área maneja un perfil de navegación específico y plenamente documentado y donde cada modificación y autorización debe pasar por gerencia antes de realizar algún ajuste de las políticas ya creadas.
- 3. POLÍTICAS DE RUTEO:** Cada una de las Vlan que están creadas están debidamente parametrizadas para que no se puedan ver entre Vlan's, y estas tienen como destino la Vlan Servidores y la interfaz SDWAN con 3 canales dedicados de internet: Internet_Canal_Movistar (wan1 100mbps) /// Internet_Canal_Claro (wan2 300mbps) /// Backup Claro (port1 300mbps); la Vlan_Servidores está enrutada a las diferentes Vlan.
- 4. AJUSTES DE SENSORES:** Como complemento al sistema Filter WEB del firewall, se realizan ajustes en los sensores de Email y data leak prevention en las Vlan de los clientes; en la Vlan_Servidores se ajustan los sensores de data leak prevention y protección de intrusos con políticas de bloqueo de objetos sospechosos en la LAN y las WAN.
- 5. VPN IPsec SSL:** Dado que pueden existir agentes trabajando In-House en la campaña del clientes, estos se conectan a **RST Asociados S.A.S** a través de una VPN con la aplicación FortiClient en su versión 5.0.2 de Windows para clientes a 32 y 64 bits donde acceden al servidor de voz para realizar gestión telefónica, se conectan a una unidad de red perteneciente a su campaña y se logea dentro de una aplicación web accediendo al servidor 172.16.10.x.x y 172.16.10.x.x que es un servidor para CRM.

2.4. SEGURIDAD FÍSICA

Parte del compromiso de **RST Asociados S.A.S** es el de velar por la seguridad y parte fundamental de la seguridad es el control que se pueda realizar en la planta física de la compañía.

Por lo tanto, se han dispuesto los siguientes elementos para asegurar la integridad de las personas y los elementos de la compañía.

- a) EDIFICIO CON VIGILANCIA:** Al estar ubicados en la zona norte de la ciudad, y los cuadrantes de la policía son vitales; además, el edificio donde

Elaborado por: Director administrativo y director de T. I	Revisado por: Director administrativo y auditor interno	Aprobado por: presidente
Fecha: 29/02/2024	Fecha: 29/02/2024	Fecha: 29/02/2024

Estamos ubicados tiene CCTV con monitoreo 24/7 y la vigilancia permanente por parte de la entidad MELTEC MOTOROLA.

- b) **CCTV:** actualmente la compañía cuenta con 8 cámaras digitales conectadas a un NVR que está publicado y filtrado por el firewall.
- c) **LECTOR DE TARJETAS:** Cada persona; empleado o visitante de **RST Asociados S.A.S**, está obligado a portar un carnet en un lugar visible, el cual tiene autorizado ciertos accesos a las diferentes áreas de la empresa.
- d) **ACTAS DE INGRESO:** En la recepción de la compañía, se toma nota del ingreso de los visitantes y se lleva control del ingreso de Dispositivos como PC's, portátiles, discos duros, tablets, dispositivos de almacenamiento de gran volumen y celulares según sea el caso, en caso de ser requerido su uso se genera el registro de autorización para uso de dispositivos móviles o celulares en el trabajo.
- e) **BITÁCORA DE INGRESO DATACENTER:** En el DataCenter se encuentra un documento aprobado por el área de SGC en la cual se registraron los datos de las personas ajenas a **RST Asociados S.A.S** que tengan contacto con esta área restringida, con el fin de llevar un seguimiento de quien ingresa, tiempo de permanencia y motivo de ingreso al DataCenter.
- f) **LOCKERS:** Se tienen lockers en un espacio vigilado por CCTV donde los agentes guardan sus elementos, incluyendo dispositivos de almacenamiento y celulares.
- g) **AUDITORÍAS EXPRESS:** Se realizan auditorias aleatorias mensuales donde el área de sistemas y calidad verifican que los celulares de los agentes se encuentren en el lugar autorizado para su almacenaje mientras permanecen en la empresa.
- h) **PLANTA ELÉCTRICA:** El lugar donde RST Asociados desarrolla su objeto comercial cuenta con un sistema de corriente alterna independiente a la acometida eléctrica del proveedor de servicio eléctrico, la cual es una planta de gran capacidad que surte de fluido eléctrico al edificio en caso de algún apagón o falla eléctrica externa; El mantenimiento de esta infraestructura es anual y programado para no afectar a nadie en el edificio.
- i) **UPS:** **RST Asociados S.A.S** cuenta en su DataCenter con una UPS de 10KVA y redundancia de 6KVA, a fin de proteger los servidores y mantenerlos en línea en caso de algún incidente eléctrico y su mantenimiento preventivo es anual y programado.
- j) **SUPRESORES DE PICOS:** Contamos con dos supresores de picos que regulan el fluido eléctrico en la zona administrativa y el Contact Center; el mantenimiento preventivo de estos dispositivos es anual y programado.
- k) **CABLEADO ESTRUCTURADO:** Tanto el cableado de datos 6a como el eléctrico es certificado bajo los estándares regulares de calidad asegurando su máxima calidad y funcionalidad.

2.5. SEGURIDAD DE LOS DATOS

	POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Clasificación: 2
		Versión: 6.0
		Fecha de Actualización: 29/02/2024

Son varios los protocolos empleados para asegurar que los datos de los clientes están protegidos en caso de cualquier evento.

Los protocolos empleados para la protección de los datos de los clientes son:

- a) **HOJA DE VIDA DE COMPUTADOR:** Se lleva una hoja de vida por equipo donde se relacionan los seriales de las partes del equipo, sus periféricos y se realizan observaciones si hay lugar a ello.
- b) **ACTA DE ENTREGA DE EQUIPOS Y CLAVES:** Se realiza la entrega de un acta en la cual se le asigna un computador y se relacionan las claves genéricas con la que el usuario ingresará al equipo y a las aplicaciones para que el usuario las cambie siendo estas claves con alfanuméricas con caracteres especiales incluidos; Cuando el usuario cambie de equipo, se registrará en una nueva acta.
- c) **ACTA DE ENTREGA DE EQUIPOS Y CIERRE DE USUARIO:** Cuando una persona culmina su contrato laboral o renuncia se levanta un acta para paz y salvo y el coordinador envía un correo al área IT para cancelar los usuarios y disponer de la máquina y eliminar los usuarios de las diferentes aplicaciones; cuando se tiene una licencia remunerada o no remunerada, permisos especiales y vacaciones, depende del coordinador avisar que se hace con los usuarios, y las máquinas.
- d) **AUDITORÍA MENSUAL DE EQUIPOS:** A través de un acta se revisan los diferentes criterios de seguridad tal como navegación de internet, accesos no autorizados, Acceso a dispositivos USB y borrado seguro de la información; los log's de borrado seguro se almacenarán y si hay alguna observación o plan de mejora se colocara en las observaciones del documento y se almacenarán de manera incremental.
- e) **ACTUALIZACIONES Y ANÁLISIS:** Las actualizaciones de sistema operativo se realizarán con la auditoria mensual de los equipos, y los antivirus se programarán para que realicen un examen rápido todos los días como tarea programada al medio día todos los días.
- f) **GPO:** Se programan las directivas locales de seguridad del sistema operativo Windows con el fin de restringir los permisos del usuario estándar para que no realice ninguna modificación en la máquina y que no acceda a lo que no tiene derecho; se restringe el acceso a impresoras, a los sitios de red, ingresar al panel de control, el menú ejecutar, a cambiar el wallpaper entre otros bloqueos necesarios para asegurar la seguridad de los datos que se manejan en la compañía.
- g) **BLOQUEO DE USB:** Se bloquean las memorias USB a través del programa Smartshield y del registro de Windows.
- h) **FILE SERVER:** Se cuenta con un servidor dedicado para ser servidor de archivos al cual cada uno de los computadores de la oficina puede ver siempre y cuando se programe la respectiva unidad de red.

Elaborado por: Director administrativo y director de T. I	Revisado por: Director administrativo y auditor interno	Aprobado por: presidente
Fecha: 29/02/2024	Fecha: 29/02/2024	Fecha: 29/02/2024

	POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Clasificación: 2
		Versión: 6.0
		Fecha de Actualización: 29/02/2024

- i) **GRABACIÓN DE 100% DE LAS LLAMADAS:** Todas las llamadas son grabadas y el área de calidad ha sido provista de herramientas para hacer Monitoreos en línea a fin de revisar no solo la gestión telefónica.
- j) **ENCRIPCIÓN DE DATOS:** A través de la herramienta GPG o la que el cliente destine para tal fin; se cifra la información interna de la empresa y la información que es enviada por correo electrónico a los clientes contratantes asegurando que la información llega de manera segura al destinatario que tiene la herramienta y la llave de descifrado que es exclusiva de **RST Asociados S.A.S.**

2.6. BACKUP DE LA INFORMACIÓN

Como parte fundamental de la seguridad de la información, se establece un procedimiento de copia de seguridad de la información.

1. **BACKUP DE LOS EQUIPOS:** De los computadores de la compañía no se hace ningún backup ya que toda la información debe estar únicamente en los servidores de la empresa.
2. **BACKUP DE SERVIDOR FILE SERVER Y AD:** Se realiza Backup de acuerdo a las políticas establecidas y al proceso creado.
3. **BACKUP SERVIDOR DEDICADO BD:** Se realiza Backup de acuerdo a las políticas establecidas y al proceso creado.
4. **BACKUP DE EMAIL:** Para este proceso no se realiza backup ya que trabajando con el sistema de Microsoft Outlook o con Mozilla Thunderbird, se almacena en el equipo un archivo con extensión .pst y en caso de pérdida de información del correo electrónico, se restaura una copia desde el web mail a través del reenvío pop de mensajes enviados y salientes.
5. **BACKUP DE SERVIDOR DE APLICACIONES:** en esta máquina se maneja la virtualización de los servidores de Monitoreo de red, plataforma de tickets, CRM Neotel, Marcador Neotel, Landing Page, Bridge BD y se realiza Backup de acuerdo a las políticas establecidas y al proceso creado.

LOS BACKUP DE LA INFORMACIÓN SE REALIZAN DE DOS FORMAS LAS CUALES SON:

El backup se genera de manera automática desde los servidores a un servidor de Backup y luego se transfiere a el servidor NAS.

2.7. BACKUP HARDWARE

El backup del hardware se realizará bajo los siguientes lineamientos.

- Llega un nuevo elemento y hay que hacer el backup de controladores.
- Se realizó un cambio y este hay que almacenarlo para llevar la bitácora.

2.8. HACKING ETICO

El hacking ético se realizará de la siguiente manera:

1. Análisis anual de vulnerabilidades de Hacking ético se realiza por un proveedor externo de manera anual.

Elaborado por: Director administrativo y director de T. I	Revisado por: Director administrativo y auditor interno	Aprobado por: presidente
Fecha: 29/02/2024	Fecha: 29/02/2024	Fecha: 29/02/2024

	POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Clasificación: 2
		Versión: 6.0
		Fecha de Actualización: 29/02/2024
<div>2. Se realiza análisis de vulnerabilidades de manera Semestral por un contratista externo</div> <div>3. Se realizará retest mensual de análisis de vulnerabilidades</div> <div>4. Cada Análisis llevará un listado de vulnerabilidades halladas y su correspondiente informe de subsanación.</div>		

Elaborado por: Director administrativo y director de T. I	Revisado por: Director administrativo y auditor interno	Aprobado por: presidente
Fecha: 29/02/2024	Fecha: 29/02/2024	Fecha: 29/02/2024

	POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Clasificación: 2
		Versión: 6.0
		Fecha de Actualización: 29/02/2024

3. POLÍTICA DE USUARIOS, CONTRASEÑAS, UTILIZACIÓN DE LA INFORMACIÓN Y VISITAS.

Cada usuario es responsable directo de la información que maneja dentro y fuera de la organización, por lo cual se establecen los siguientes criterios de seguridad, con el fin de asegurar que la información dentro de **RST Asociados S.A.S** está segura y tiene un tratamiento organizado y estructurado.

3.1. POR FUERA DE LA COMPAÑÍA

Los usuarios tienen completamente prohibido suministrar información con relación a clientes, usuarios, transacciones o demás procesos que se deriven de su labor al interior de la compañía; por lo cual se establecen cláusulas de confidencialidad en sus contratos de trabajo.

- Los usuarios deben firmar un acuerdo adicional de confidencialidad de la información.
- Los usuarios deben firmar un acuerdo adicional de protección de los datos de carácter confidencial de la información y de la operación.
- Los usuarios no tendrán por fuera de las instalaciones de la compañía ningún acceso remoto que les permita ingresar a servicios de voz o datos.
- Los usuarios que tengan asignado un correo electrónico de la compañía para hacer la gestión con los clientes asignados tienen prohibido el acceso a este sistema; el acceso por web mail está únicamente autorizado para el director del área IT de **RST Asociados S.A.S**.

Se establece las siguientes normas para el uso del correo electrónico, con el fin de evitar afectación en la seguridad de la información para las actividades que se realizan por **RST Asociados S.A.S.**, como es:

1. Sé breve, vete al titular (hay que ir al grano; no estamos para hacer literatura).
2. Envía los correos electrónicos a las personas que realmente los necesitan y no remitir o responder correos a usuarios spam o no deseados; tampoco acceder a enlaces desconocidos o sospechosos.
3. Durante la realización de las labores asignadas para la operación, no acceder al correo personal.
4. Puntualiza claramente el objetivo del mensaje y qué esperas del receptor (no te olvides del asunto).
5. Sitúa lo más importante al principio (no des por hecho que van a leer todo tu correo).
6. Cuida siempre el lenguaje (nunca sabes a dónde puede ir a parar tu mensaje).
7. No descuides tampoco la ortografía ni la gramática (no eres tú solo el que escribe, sino que representas a tu empresa).
8. Trabaja y cuida el tono de tus correos (para evitar que se malinterprete).
9. Plantea preguntas de respuesta breve (así obtendrás mayor feedback).
10. Evita incluir documentos adjuntos muy pesados (es preferible enlazar).
11. Saca todo el rendimiento a la tecla “suprimir”. Atrévete. No todo hay que responderlo.

3.2. AL INTERIOR DE LA COMPAÑÍA

- a) Los usuarios deben firmar hoja de vida del computador asignado dónde está relacionado que se le está entregando.

Elaborado por: Director administrativo y director de T. I	Revisado por: Director administrativo y auditor interno	Aprobado por: presidente
Fecha: 29/02/2024	Fecha: 29/02/2024	Fecha: 29/02/2024



POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Clasificación: 2

Versión: 6.0

Fecha de Actualización:
29/02/2024

- b) El usuario debe portar su carnet de identificación que lo acredita como trabajador de la compañía en un lugar visible.
- c) Los carnets de acceso que no estén en uso deben reposar en la tesorería donde se encuentra la caja fuerte de la compañía y la relación de estos, debe permanecer en recursos humanos.
- d) Los usuarios firman un documento llamado “Política de copia de archivos” donde se lleva una bitácora de los archivos almacenados en medios magnéticos o digitales previa autorización del jefe directo del área con el fin de prevenir la fuga de la información.
- e) Los usuarios no deben guardar información personal y/o laboral en el escritorio, en la carpeta “mis documentos” o alguna otra ubicación dentro del ordenador ya que para tal fin, a cada usuario se le asignara una unidad de red única o compartida para la campaña según sea el caso.
- f) El personal contratado debe contar con un estudio de seguridad el cual puede realizarse con llamadas a sus referencias familiares, personales y laborales; la consulta de sus antecedentes disciplinarios o la consulta ante la procuraduría general de la nación para asegurarnos que el empleado es idóneo a nivel de seguridad para la labor que es contratado.
- g) Los usuarios deben firmar documento de administración de PC’S donde se le informa al usuario la política de buen uso del computador la cual se describe a continuación:
 - Uso responsable de páginas web (las cuales según los privilegios se le otorga y/o deniega el acceso a tal vez de los web Filter del firewall).
 - Descarga o instalación de software.
 - Copia y descarga de música, videos, documentos y demás archivos que no sean de orden corporativo.
 - Está prohibida la instalación de fondos de pantalla y protectores de pantalla que no sean los autorizados por **RST Asociados S.A.S.**
 - Cada usuario es responsable de su ID de usuario que es único y su contraseña de inicio de sesión la cual es única por lo que no la debe suministrar a ningún compañero de trabajo o externo a la compañía.
- h) El nivel de complejidad de las contraseñas asignadas para los usuarios es alto, por lo que debe contar mínimo con 8 caracteres alfanuméricos incluyendo mayúsculas y mínimo debe tener un carácter especial (Entiéndase carácter especial como &%\$#;,;.”@).

3.3. EL PERSONAL VISITANTE

Elaborado por: Director administrativo y director de T. I	Revisado por: Director administrativo y auditor interno	Aprobado por: presidente
Fecha: 29/02/2024	Fecha: 29/02/2024	Fecha: 29/02/2024

	POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Clasificación: 2
		Versión: 6.0
		Fecha de Actualización: 29/02/2024

El personal ajeno a RST Asociados, el cual no tenga contrato con la compañía se le denominara visitante; este visitante puede tener 5 perfiles que son:

- a) Cliente directo de unidad de negocio.
- b) Cliente de operación (Atención al cliente por procesos propios de la operación si hay lugar a ello).
- c) Soporte técnico o proveedor de servicios de **RST Asociados S.A.S.**
- d) Personal de mensajería.
- e) Personal in particular (Familiar etc.).

Por esto mismo, **RST Asociados S.A.S** establece una política para la atención de las visitas en la compañía.

CLIENTE DIRECTO: Este debe portar carnet en lugar visible de la compañía que lo acredite como trabajador De la compañía, tendrá acceso a los espacios destinados para su atención y en todo momento debe estar acompañado de las personas que intervienen en el proceso; debe firmar acta de ingreso en la recepción y registrarse con sus datos personales, incluso debe registrar equipos de cómputo si los trae.

CLIENTE DE OPERACIÓN: Este visitante deberá ser atendido en la recepción de la compañía y no podrá acceder a otros espacios de la misma únicamente bajo autorización de una jefatura según sea el proceso, esto será tratado como una excepción y se le debe solicitar a las personas que tengan su celular en vibrador y abstenerse de comunicarse por el mientras permanezca en las instalaciones de la compañía.

SOPORTE TÉCNICO O PROVEEDOR DE SERVICIOS: Este visitante deberá registrarse en el libro de visitas que se encuentra en la recepción y en todo momento debe estar acompañado por la persona que intervenga en su proceso; podrá contestar su celular mientras permanezca en la compañía pero solo mientras la comunicación sea dedicada a la labor de su visita.

PERSONAL DE MENSAJERÍA: Estos visitantes no podrán acceder sino hasta la recepción y el destinatario motivo de su visita debe atenderlo en este lugar, está prohibido que el personal se acerque a cualquier área de la compañía y siempre debe portar un carnet que lo acredite como funcionario de la entidad de mensajería.

PERSONAL PARTICULAR: Este tipo de personal puede ingresar a la compañía con la autorización expresa de recursos humanos, se debe apuntar en el libro de visitas, registrar los computadores si los trae y debe colocar su celular en silencio; está terminantemente prohibido que el personal visitante a la compañía, acceda a las dependencia de acceso restringido y siempre debe estar acompañado de la persona, trabajador de RST que se debe hacer responsable de la permanencia y los actos realizados por el visitante.

3.4. CLASIFICACIÓN DE LA INFORMACIÓN CORPORATIVA

Elaborado por: Director administrativo y director de T. I	Revisado por: Director administrativo y auditor interno	Aprobado por: presidente
Fecha: 29/02/2024	Fecha: 29/02/2024	Fecha: 29/02/2024



POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Clasificación: 2

Versión: 6.0

Fecha de Actualización:
29/02/2024

Según la naturaleza de la información que RST Asociados maneja con sus clientes y proveedores se determinan varios niveles de información, para los cuales existe un protocolo de calidad, disponibilidad, confidencialidad e integralidad que los activos de información deben tener con el fin de cumplir con procesos de seguridad de la información.

Estos niveles son:

- a) **INFORMACIÓN PÚBLICA:** En esta se incluyen todos los datos de dominio público y cuyas características principales deben ser la objetividad y la disponibilidad, ya que es información a la que pueden acceder los clientes y proveedores de manera abierta, su naturaleza no lleva implícita mayor protocolo que el de asegurar su custodia y su correcta difusión por lo que es competencia del asignado a cada proceso, velar por que la información tenga una correcta utilización y de no ser así debe hacerse merecedor de sanciones so pena del nivel de criticidad y afectación que esto pueda acarrear a la compañía.
- b) **INFORMACIÓN DE USO INTERNO:** En esta se contiene toda la información que sea de posible intercambio en la empresa la cual que se convierte estructura principal de la operación del negocio; por lo tanto las características implícitas a este tipo de información son las de disponibilidad e integridad, por lo que debe estar sujeta a políticas de backup de la información y a cláusulas de confidencialidad dentro de los contratos en el personal que tenga acceso a este tipo de información.
- c) **INFORMACIÓN DE USO CONFIDENCIAL:** Directamente Equivalente con una naturaleza de origen reservado; por ejemplo; planes de negocio, información de nuevos productos y servicios, resultados de investigaciones o actividades relacionadas directamente con entrega de información a clientes.

Elaborado por: Director
administrativo y director de T. I

Fecha: 29/02/2024

Revisado por: Director administrativo
y auditor interno

Fecha: 29/02/2024

Aprobado por: presidente

Fecha: 29/02/2024



POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Clasificación: 2

Versión: 6.0

Fecha de Actualización:
29/02/2024

La principal característica de este tipo de información es su confidencialidad. Como esta información puede contener datos sensibles como nombres, números de cedula, direcciones y teléfonos u otros datos derivados al objeto de la gestión realizada sobre una operación, se debe contar con herramientas de cifrado de la información las cuales deben ser de común acuerdo con el cliente implantadas y de ser necesario levantar acta del proceso para ambas partes con el fin de asegurar un proceso de calidad y de seguridad de la información.

Según el nivel y el proceso, la información que se maneja al interior de la compañía o la que sale de ella para los clientes debe cumplir con los siguientes criterios.

- d) **BORRADO SEGURO:** Según lo determine cada cliente, se deben aplicar herramientas de software para borrar de manera lógica, la información en cierto rango de tiempo; Este proceso debe estar soportado por un acta de eliminación de la información en la cual interviene el director del proceso, el agente o analista del proceso y el director de IT y debe quedar documentada como registro verídico de la actividad realizada.
- e) **ELIMINACIÓN DE ELEMENTOS FÍSICOS:** Se debe destruir de la misma manera los documentos en papel como copias, faxes, correos electrónicos impresos, medios magnéticos como CDs, cartas de autorizaciones y demás elementos en papel que se deriven, fruto de la gestión realizada para el cliente, su proceso de eliminación y destrucción se debe realizar en una picadora de papel y la custodia de esta información debe acordarse dentro de la política de servicios entre el cliente y la compañía.
- f) **BACKUP DE LA INFORMACIÓN:** Según la sensibilidad del activo de información se debe realizar un backup de la información bajo los siguientes premisas:
 - **PUBLICA:** Debe realizarse mensual o cada vez que exista un cambio sustancial dentro del activo.
 - **CRÍTICA:** Información confidencial o de uso diario con la cual se realice una gestión operacional debe tener un backup diario.
 - **HISTÓRICA:** Información que debe asegurarse por labores mismas de la gestión operacional y que solo puede ser eliminada cuando pierda su validez o cuando el cliente en si lo requiera; su backup debe hacerse en un medio magnético cifrado y almacenado en caja fuerte.
- g) **SEGMENTACIÓN DE LA INFORMACIÓN:** La información debe estar bajo la directa responsabilidad de una sola persona y en sus recursos corporativos se debe velar por que únicamente tenga acceso a la información que le corresponde.
- h) **SEGURIDAD DE LA INFORMACIÓN:** La persona estará sujeta a políticas de filtrado web y al bloqueo de unidades de unidades tanto flash como de unidades ópticas para evitar la fuga de la información; En la estructura de seguridad de la compañía, el firewall también debe tener políticas de Data Leak prevention con el fin de asegurarse que el agente o el analista no pueda controlar esta información sino solo para el bien corporativo y no para bien propio.

3.5. CIFRADO DE LA INFORMACIÓN

Elaborado por: Director
administrativo y director de T. I

Fecha: 29/02/2024

Revisado por: Director administrativo
y auditor interno

Fecha: 29/02/2024

Aprobado por: presidente

Fecha: 29/02/2024



POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Clasificación: 2

Versión: 6.0

Fecha de Actualización:
29/02/2024

El cifrado es un procedimiento, en el cual se utilizan algoritmos para transformar la información en un elemento ilegible; para transformar el archivo y convertirlo en un archivo legible, es necesario contar con una llave o contraseña de descifrado a fin de convertir el archivo en un elemento legible.

Se establece por política que para garantizar la integridad de la información que se envía o se recibe del cliente, siempre y por sobre todo concepto, esta debe venir cifrada con algún tipo de mecanismo.

Este mecanismo de cifrado se debe acordar directamente con el cliente ya que debemos asegurarnos en que la información viaje segura; pero asegurándonos que también el cliente sea el que tenga la autonomía de elegir la herramienta con la cual se proteja la información.

Internamente contamos con la herramienta PGP con una llave de cifrado exclusiva de RST pero es el cliente al final quien decide si se incorpora o no. La información se debe cifrar bajo las siguientes circunstancias:

- a) Se van a enviar archivos por correo electrónico (documento adjunto cualquiera que sea su extensión) con el fin de que la información viaje segura.
- b) Información almacenada en medios de almacenamiento USB o medio magnético como CD, DVD, Blu-ray, disco 3 ½ o cintas.

El proceso de encriptación va de acuerdo a la herramienta con la que los clientes de RST Asociados determinen que se deba realizar el proceso, bien sea por algún canal FTP, Acceso web de comunicación segura o software como Winrar, WinZip, Adobe Acrobat pro, PGP, cipher o cualquier existente en el mercado.

En la interfaz de GPG se debe abrir el programa y con la clave de descripción establecida de debe generar la opción de cifrar la información.

Desde Winrar o WinZip al archivo se le debe dar Click derecho (Interfaz Windows de Microsoft), seleccionar la opción de añadir al archivo con el icono del programa y en la opción de contraseña se debe colocar una contraseña mínimo con 8 caracteres alfa numéricos incluyendo mayúsculas y mínimo debe tener un carácter especial (Entiéndase carácter especial como & % \$ # , ; . Ä " @) o la que el cliente determine para tal fin.

Elaborado por: Director
administrativo y director de T. I

Fecha: 29/02/2024

Revisado por: Director administrativo
y auditor interno

Fecha: 29/02/2024

Aprobado por: presidente

Fecha: 29/02/2024

4. INCIDENCIAS						
4.1. REPORTE DE INCIDENCIAS						
Todos los reportes de incidencias se deben realizar por la plataforma de tickerts, con el fin de recibir trazabilidad por este mismo medio y tener la evidencia del proceso. Estos son los tiempos de respuesta para cada uno de los eventos que puedan presentarse al interior de la compañía.						
EVENTO	NIVEL DE SERVICIO				TDR	OBSERVACIONES
	BAJ	MED	ALT	CRIT		
CAMBIO Y / O SOPORTE DE DIADEMA	X				4 HORAS	Depende de las existencias o del nivel crítico de inoperancia.
CAMBIO Y / O SOPORTE DE MOUSE	X				4 HORAS	Depende de las existencias o del nivel crítico de inoperancia.
CAMBIO Y/O SOPORTE DE TECLADO	X				4 HORAS	Depende de las existencias o del nivel crítico de inoperancia.
CAMBIO Y/O SOPORTE DE PANTALLA		X			1 HORA	Depende de las existencias o del nivel crítico de inoperancia.
CAMBIO DE EQUIPO	X				1 DÍA	Se debe programar con un día de anterioridad la movilización del ordenador.
FUNCIONAMIENTO LENTO DEL PC	X				4 HORAS	Dependiendo del nivel de inoperancia se realizará mantenimiento preventivo y de no funcionar se procederá a realizar cambio de equipo.
FALLA EN SOFTPHONE			X		15 MINUTOS	Se revisará y se solucionará el inconveniente; de seguir presentándose la falla se creará un ticket de seguimiento hasta que se solucione el problema.
FALLA CORREO ELECTRONICO	X				8 HORAS	Se determinarán fallas en Outlook, se realizará mantenimiento preventivo y correctivo.
CREACION CORREO ELECTRONICO	X				1 DÍA	Depende de las existencias en el hosting.

ASIGNACION DE EXTENSIONES Y USUARIOS	X				1 DÍA	Debe ser un tema programado.
FIRMA DE CORREO ELECTRONICO	X				1 HORA	Se debe enviar un correo electrónico a soporte con todos los datos de la persona a la que se le va a crear la firma para incluirlos en la imagen.
MANTENIMIENTO PREVENTIVO DE PC	X				1 DÍA	Debe ser una tarea programada.
MANTENIMIENTO PREVENTIVO DE SERVIDORES			X		1 DÍA	Debe ser una tarea programada y no habrá operación del servidor, también debe ser un soporte de un día por cada servidor.
MANTENIMIENTO CORRECTIVO DE PC			X		1 HORA	Se realizará soporte de mantenimiento de pc, depende del soporte se asignará un nuevo pc según stock en caso de falla inminente.
MANTENIMIENTO CORRECTIVO DE SERVIDORES				X	INMEDIATO	El tiempo de recuperación de la operación dependerá de la falla del sistema.
MANTENIMIENTO DE APLICACIONES		X			4 HORAS	Se realizará soporte de primer nivel y de presentarse una falla de carácter mayor, se procederá a realizar los respectivos direccionamientos a los proveedores.

	POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN					Clasificación: 2
						Versión: 6.0
						Fecha de Actualización: 29/02/2024

MANTENIMIENTO PREVENTIVO DE LA RED		X			5 HORAS	Debe ser una tarea programada y no habrá operación.
MANTENIMIENTO CORRECTIVO DE LA RED				X	INMEDIATO	El tiempo de recuperación de la operación dependerá de la falla del sistema.
CAIDAS DE INTERNET				X	INMEDIATO	Se solicitará soporte al proveedor de ISP.
FALLAS EN OFFICE	X				4 HORAS	Se aplicarán parches, de continuar el problema se creara un ticket de seguimiento hasta que se solucione el problema.
FALLA EN TRANSFERENCIA DE LLAMADAS		X			2 HORAS	Se aplicará una recarga de la planta y se monitoreara la operación por una hora para determinar fallas internas y descartar fallas en las líneas.
CORTE DE LLAMADAS				X	INMEDIATO	Se revisara el PBX y se ayudara a determinar el origen de la falla, cuando son a números fijos se revisara la planta telefónica y se solicitara soporte al proveedor de ISP y de PBX; cuando sean fallas a telefonía celular se enviara solicitud de soporte a proveedor de SIP TRUNK el cual dependerá que el solicitante envíe un correo con los números de rastreo para que sea determinado el origen de la falla, al igual se sienta precedente de que la calidad y estabilidad en la comunicación celular no depende de RST sino en un porcentaje del 15% del proveedor de SIP TRUNK y el 85% de los operadores de telefonía celular.
MANTENIMIENTO FIREWALL				X	INMEDIATO	Diariamente este dispositivo es monitoreado así que en caso de caída, los protocolos de soporte son aplicados de inmediato.

Elaborado por: Director administrativo y director de T. I	Revisado por: Director administrativo y auditor interno	Aprobado por: presidente
Fecha: 29/02/2024	Fecha: 29/02/2024	Fecha: 29/02/2024

	POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN					Clasificación: 2
						Versión: 6.0
						Fecha de Actualización: 29/02/2024

FALLAS VPN			X		1/2 HORA	Se realizará soporte solicitado.
DIAS DE PAGO DE NOMINA			X		1/2 HORA	Recibirá soporte con las entidades financieras con las que RST trabaje.
GRABACIONES	X				3 DÍAS HABLES	Se realizará el descargue de las grabaciones por programación bajo solicitud realizada por correo electrónico cuando son de carácter masivo.
GRABACION EN UNIDADES OPTICAS		X			1 HORA	Deben solicitar el tema por correo electrónico y deben remitir al área de sistemas los medios magnéticos para realizar el respectivo soporte.

En caso de presentarse algún evento que no esté relacionado en el presente listado; se debe contar con la existencia del correo electrónico con el fin de poder realizar el seguimiento de la incidencia.

5. AUDITORÍAS INTERNAS Y DE CALIDAD PARA LA SEGURIDAD DE LA INFORMACIÓN.

El área de sistema de gestión de calidad de la compañía programa y realiza con frecuencia mensual una verificación de los equipos de cómputo donde se revisan los siguientes conceptos:

- a) Acceso no autorizado a dispositivos USB, cd, DVD, Blu-ray.
- b) Acceso no autorizado a páginas de internet.
- c) Recursos de red: que solo pueda acceder a su unidad de red asignada.
- d) Imágenes corporativas en el escritorio y screensaver.

DESPUÉS DE ESTO SE REALIZAN TAREAS DE:

- a) Mantenimiento preventivo del pc.
- b) Instalación de actualizaciones antivirus.
- c) Instalación de seguridad de actualizaciones Windows Update (productos Microsoft)
- d) Actualizaciones de versiones open Office (Contact Center).

Para esto la compañía ha dispuesto un PC con el fin de realizar las pruebas en la instalación de las respectivas actualizaciones con el fin de evaluar temas de rendimiento, por lo que si se nota algún factor que influya negativamente a la maquina en temas de desempeño, será omitida esa actualización hasta que exista un nuevo parche de seguridad que pueda ser instalado y que no afecte el rendimiento de la máquina.

Si hay un evento de seguridad, se debe colocar en las observaciones del documento que hallazgos se encontraron y se debe proceder en los próximos 3 días (Dependiendo de la criticidad del hallazgo) se debe realizar un acta donde se describa la solución del problema.

El Director del SGC programa y realiza con una frecuencia anual auditorías internas al SGC y SGSI para verificar la eficacia de los procesos, prestación del servicio, y controles establecidos en seguridad de la información.

Elaborado por: Director administrativo y director de T. I	Revisado por: Director administrativo y auditor interno	Aprobado por: presidente
Fecha: 29/02/2024	Fecha: 29/02/2024	Fecha: 29/02/2024

	POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Clasificación: 2
		Versión: 6.0
		Fecha de Actualización: 29/02/2024

6. PLAN DE CONTINUIDAD DEL NEGOCIO
6.1. PLAN DE BCP
<p>El objetivo del business continuity plain o plan de continuidad de negocio, es aumentar la probabilidad de continuidad de las funciones críticas de la organización en caso de que un incidente interrumpa las operaciones informáticas, como también proporcionar una respuesta rápida y apropiada a cualquier incidente imprevisto que pueda afectar las instalaciones físicas, la infraestructura tecnológica, la información y el personal en la operación de RST Asociados S.A.S.</p> <p>El alcance de este plan guarda relación con la infraestructura informática, la respuesta a emergencias, el manejo de crisis y recuperación de procesos, así como los procedimientos relevantes asociados con la plataforma tecnológica. Los procedimientos relevantes a la infraestructura informática son aquellas tareas que el personal realiza frecuentemente al interactuar con la plataforma informática (entrada de datos, generación de reportes, consultas, etc.), esto con el fin de que RST Asociados S.A.S no se vea afectada en la prestación del servicio.</p> <p>Con el fin de verificar la eficacia en lo establecido para el Plan de BCP se realiza una prueba anual para determinar si es necesario realizar ajustes en los procedimientos establecidos.</p>
6.2. ROLES BCP, ORGANIZACIÓN DE LOS EQUIPOS.
<p>Los equipos de emergencia están formados por el personal clave necesario en la activación y desarrollo del Plan de Continuidad. Cada equipo tiene unas funciones y procedimientos que tendrán que desarrollar en las distintas fases del Plan.</p> <p>Aunque la composición y número de equipos puede variar según el tipo de estrategia de recuperación, a continuación se muestran algunos ejemplos de los equipos que pueden formar parte del Plan:</p> <ul style="list-style-type: none"> a) COMITÉ DE CRISIS: Encargado de dirigir las acciones durante la contingencia y recuperación. b) EQUIPO DE RECUPERACIÓN: Su función es restablecer todos los sistemas necesarios (voz, datos, comunicaciones, etc.). c) EQUIPO LOGÍSTICO: Responsable de toda la logística necesaria en el esfuerzo de recuperación. d) EQUIPO DE LAS UNIDADES DE NEGOCIO: Encargados de la realización de pruebas que verifiquen la recuperación de los sistemas críticos. e) EQUIPO DE RELACIONES PÚBLICAS: Encargado de las comunicaciones a los medios de comunicación y clientes. <p>El personal asignado a cada uno de los equipos puede variar dependiendo del tamaño de la organización y de la estrategia de recuperación seleccionada. Una persona puede pertenecer a más de un equipo, siempre y cuando no existan incompatibilidades en las tareas a realizar.</p> <p>EQUIPO DIRECTOR O COMITÉ DE CRISIS</p>

Elaborado por: Director administrativo y director de T. I	Revisado por: Director administrativo y auditor interno	Aprobado por: presidente
Fecha: 29/02/2024	Fecha: 29/02/2024	Fecha: 29/02/2024

	POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Clasificación: 2
		Versión: 6.0
		Fecha de Actualización: 29/02/2024

El objetivo de este comité es reducir al máximo el riesgo y la incertidumbre en la dirección de la situación. Este Comité debe tomar las decisiones “clave” durante los incidentes, además de hacer de enlace con la dirección de la compañía, manteniéndolos informados de la situación regularmente.

Las principales tareas y responsabilidades de este comité son:

- a) Análisis de la situación.
- b) Decisión de activar o no el Plan de Continuidad.
- c) Iniciar el proceso de notificación a los empleados a través de los diferentes responsables.
- d) Seguimiento del proceso de recuperación, con relación a los tiempos estimados de recuperación.

EQUIPO DE RECUPERACIÓN

El equipo de recuperación es responsable de establecer la infraestructura necesaria para la recuperación. Esto incluye todos los servidores, PC's, comunicaciones de voz y datos y cualquier otro elemento necesario para la restauración de un servicio.

EQUIPO LOGÍSTICO

Este equipo es responsable de todo lo relacionado con las necesidades logísticas en el marco de la recuperación, tales como:

- Transporte de material y personas (si es necesario) al lugar de recuperación.
- Suministros de oficina.
- Comida.
- Reservas de hotel, si son necesarias.
- Contacto con los proveedores.

Este equipo debe trabajar conjuntamente con los demás, para asegurar que todas las necesidades logísticas sean cubiertas.

EQUIPO DE RELACIONES PÚBLICAS Y ATENCIÓN A CLIENTES

Se trata de canalizar la información que se realiza al exterior en un solo punto para que los datos sean referidos desde una sola fuente. Sus funciones principales son:

- Elaboración de comunicados para la prensa.
- Comunicación con los clientes.

Elaborado por: Director administrativo y director de T. I	Revisado por: Director administrativo y auditor interno	Aprobado por: presidente
Fecha: 29/02/2024	Fecha: 29/02/2024	Fecha: 29/02/2024



POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Clasificación: 2

Versión: 6.0

Fecha de Actualización:
29/02/2024

Uno de los valores más importantes de una compañía son sus clientes, por lo que es importante mantener informados a los mismos, estableciendo canales de comunicación.

EQUIPO DE LAS UNIDADES DE NEGOCIO

Estos equipos estarán formados por las personas que trabajan con las aplicaciones críticas, y serán los encargados de realizar las pruebas de funcionamiento para verificar la operatividad de los sistemas y comenzar a funcionar.

Cada equipo deberá configurar las diferentes pruebas que deberán realizar para los sistemas.

DESARROLLO DE PROCEDIMIENTOS

Una vez que hemos definido los equipos y se han establecido las funciones que debe desempeñar cada equipo, tenemos que desarrollar los procedimientos que van a seguir, y su actuación en cada una de las fases de activación del Plan de Continuidad.

1. FASE DE ALERTA

- Procedimiento de notificación del desastre.
- Procedimiento de lanzamiento del Plan
- Procedimiento de notificación de la puesta en marcha del Plan a los equipos implicados.

2. FASE DE TRANSICIÓN

- Procedimiento de concentración de equipos.
- Procedimiento de traslado y puesta en marcha de la recuperación.

3. FASE DE RECUPERACIÓN

- Procedimientos de restauración.
- Procedimientos de soporte y gestión.

4. FASE DE VUELTA A LA NORMALIDAD

- Análisis del impacto.
- Procedimientos de vuelta a la normalidad.

En el siguiente esquema podemos ver las fases que componen el Plan de Continuidad de Negocio:

Elaborado por: Director administrativo y director de T. I	Revisado por: Director administrativo y auditor interno	Aprobado por: presidente
Fecha: 29/02/2024	Fecha: 29/02/2024	Fecha: 29/02/2024

FASE DE ALERTA

La Fase de Alerta define los procedimientos de actuación ante las primeras etapas de un suceso que implique la pérdida parcial o total de uno o varios servicios críticos. Dividiremos esta fase en tres partes:

- **Notificación:** Define cómo y quién debe ser informado en primera instancia de lo ocurrido.
- **Evaluación:** Análisis de la situación y valoración inicial de los daños. Definición de estrategias.
- **Ejecución del Plan:** Decisión del equipo director de disparar el Plan debido al alcance de los daños.

NOTIFICACIÓN

Dado que no es posible confeccionar un Plan de Alerta que dé cabida a todos los casos que resultan de suponer que cualquier persona pueda dar aviso de un incidente, vamos a suponer que la persona que descubre la contingencia será un empleado o cualquier otra persona próxima al lugar donde ocurre el incidente. Como parte del Plan de Continuidad se debe establecer un programa de concienciación, en el que se informe debidamente al personal de cómo actuar ante estos casos y a quién comunicar lo ocurrido.

EVENTO	ACCIÓN
Situación de contingencia/incidente detectado por algún empleado de la compañía. (Fuego, inundación, virus, etc.).	Aviso inmediato con el máximo detalle posible al Responsable de Personal de turno o a Seguridad.
El responsable de turno o de seguridad conoce que ha sucedido una contingencia.	Aviso a la persona de contacto del Comité de Crisis. Aviso a los equipos de emergencia (si procede).

EVALUACIÓN

Una vez que un miembro del Comité de Crisis es contactado e informado del incidente, procederá a evaluar la situación con la recopilación de la mayor información posible. El Comité informará a los responsables de los distintos equipos de lo ocurrido y de la situación en ese momento para que permanezcan en situación de espera, hasta que se tome la decisión de disparar el Plan o iniciar otro tipo de estrategia.

EVENTO	ACCIÓN
--------	--------

Conocimiento por algún miembro del Comité del incidente ocurrido.	<p>El equipo del Comité se reunirá en un lugar acordado previamente y evaluará la situación. Este Comité deberá tomar la decisión de activar o no el Plan de Continuidad. Será necesario informar de la situación a los siguientes responsables:</p> <ul style="list-style-type: none">- Responsable de Seguridad.- Comité de Dirección de la Empresa.- Relaciones Públicas.- Equipo de Recuperación.- Responsable de los Equipos.
---	--

EJECUCIÓN DEL PLAN

Una vez que el Comité de Crisis ha decidido poner en marcha el Plan de Recuperación, debe de iniciarse el Árbol de llamadas (En el Anexo IV se incluye un ejemplo de un árbol de llamadas) para comunicar a los Responsables y componentes de cada equipo la situación de inicio de las actividades del Plan para comenzar los procedimientos de actuación de cada uno de ellos. Deberá informarse también al Comité de Dirección.

EVENTO	ACCIÓN
Consideración por parte del Comité de Crisis y ejecución del Plan.	Iniciar el árbol de llamadas. Informar al Comité de Dirección.
Paso a la Fase de Transición.	

FASE DE TRANSICIÓN

La Fase de Transición es la fase previa a la recuperación de los sistemas. Es importante que en esta fase exista una coordinación entre los diferentes equipos y equipos de logística, ya que son éstos los encargados de que todo esté disponible para comenzar la recuperación en el menor tiempo posible. Podemos dividir la fase de transición en dos partes principalmente:

- Procedimientos de concentración y traslado de personas y equipos.
- Procedimientos de puesta en marcha del centro de recuperación.

PROCEDIMIENTOS DE CONCENTRACIÓN Y TRASLADO DE MATERIAL Y PERSONAS

Dependiendo de la solución final que se decida como estrategia de respaldo, este procedimiento puede variar. Realizaremos una descripción general de los procedimientos, que podrá completarse una vez que se tome una solución definitiva.

Una vez avisados los equipos y puesto en marcha el Plan, deberán acudir al centro de reunión. En el caso de que la emergencia se declare en horas de trabajo, se tomará como punto de encuentro los lugares designados en el Plan de Emergencia. Si el incidente ocurre fuera del horario de trabajo, el lugar de reunión será el designado como centro de respaldo, o cualquier otro designado por el Comité de Dirección de Crisis.

Además del traslado de personas al centro de recuperación (si es necesario) hay que realizar una importante labor de coordinación para el traslado de todo el material necesario para poner en marcha el centro de recuperación (cintas de backup, material de oficina, documentación, etc.)

PROCEDIMIENTOS DE PUESTA EN MARCHA DEL CENTRO DE RECUPERACIÓN

Una vez concentrados los distintos equipos que van a intervenir en la recuperación, y con todos los elementos necesarios disponibles para comenzar la recuperación, hay que poner en marcha este centro, estableciendo la infraestructura necesaria, tanto de software como de comunicaciones, etc.

FASE DE RECUPERACIÓN

Una vez que hemos establecido las bases para comenzar la recuperación, se procederá a la carga de datos y a la restauración de los servicios críticos. Este proceso y el anterior suele precisar los mayores esfuerzos e intervenciones para cumplir con los plazos fijados. Podemos dividir esta fase en dos:

- Procedimientos de Restauración
- Procedimientos de Gestión y Soporte

	POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Clasificación: 2
		Versión: 6.0
		Fecha de Actualización: 29/02/2024

PROCEDIMIENTOS DE RESTAURACIÓN

Estos procedimientos se refieren a las acciones que se llevan a cabo para restaurar los sistemas críticos.

PROCEDIMIENTOS DE SOPORTE Y GESTIÓN

Una vez restaurados los sistemas hay que comprobar su funcionamiento, realizar un mantenimiento sobre los mismos y protegerlos, de manera que se reanude el negocio con las máximas garantías de éxito. Los integrantes del equipo de unidades de negocio serán los encargados de comprobar y verificar el correcto funcionamiento de los procesos.

FASE DE VUELTA A LA NORMALIDAD / FIN DE LA EMERGENCIA

Una vez con los procesos críticos en marcha y solventada la contingencia, debemos plantearnos las diferentes estrategias y acciones para recuperar la normalidad total de funcionamiento. Para ello vamos a dividir esta fase en diferentes procedimientos:

- Análisis del impacto.
- Procedimientos de vuelta a la normalidad

ANÁLISIS DEL IMPACTO

El análisis de impacto pretende realizar una valoración detallada de los equipos e instalaciones dañadas para definir la estrategia de vuelta a la normalidad.

PROCEDIMIENTOS DE VUELTA A LA NORMALIDAD

Una vez determinado el impacto deben establecerse los mecanismos que en la medida de lo posible lleven a recuperar la normalidad total de funcionamiento. Estas acciones incluyen las necesidades de compra de nuevos equipos, mobiliario, material, etc.

GENERACIÓN DE INFORMES Y EVALUACIÓN

Una vez solventado el incidente y vuelto a la normalidad, cada equipo deberá realizar un informe de las acciones llevadas a cabo y sobre el cumplimiento de los objetivos del Plan de Continuidad, los tiempos empleados, dificultades con las que se encontraron, etc.

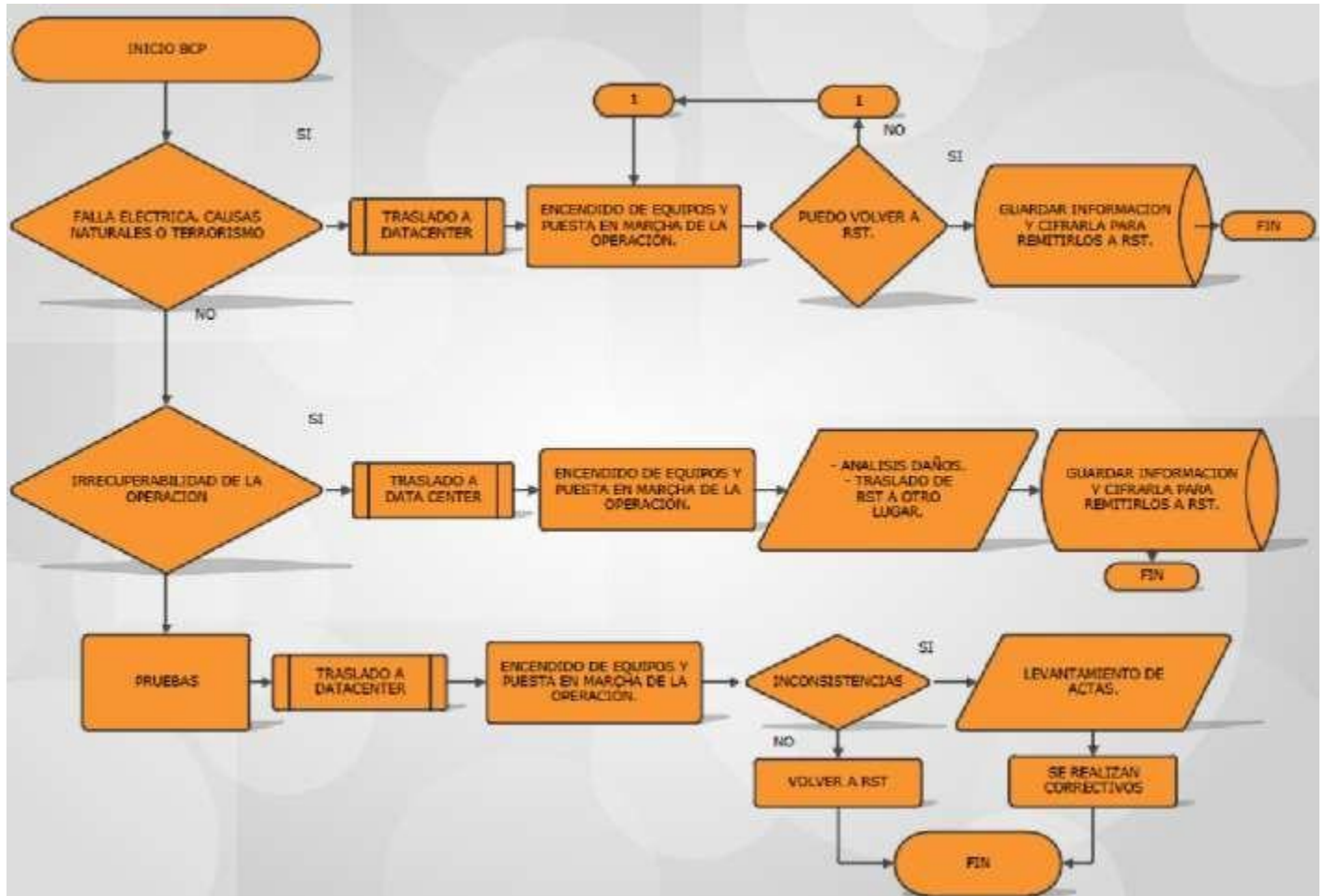
Toda esta información servirá para valorar si el Plan ha funcionado según lo planeado, así como conocer los posibles fallos, y en su caso, tenerlos en cuenta para la adecuación del mismo.

6.3. WORKFLOW DEL BCP.

Elaborado por: Director administrativo y director de T. I	Revisado por: Director administrativo y auditor interno	Aprobado por: presidente
Fecha: 29/02/2024	Fecha: 29/02/2024	Fecha: 29/02/2024

FLUJO DE PROCESOS

El plan de continuidad de negocio se encuentra detallado en el proceso BCP el cual tiene su documento aparte ya que es un proceso paralelo que RST ejecuta para garantizar la recuperabilidad de la operación en caso de algún incidente.



6.4. EXCEPCIONES.

	POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Clasificación: 2
		Versión: 6.0
		Fecha de Actualización: 29/02/2024

Este procedimiento aplica para excepciones a la presente política de la seguridad de la información; ya que hay ciertos procesos donde por cuestiones dinámicas del objeto del cumplimiento de las tareas asignadas por los clientes, se puede generar una flexibilidad a las normas establecidas.

Estas excepciones van ligadas al cumplimiento de una tarea esporádica o a una nueva labor especial y constante que se realizara con el personal de la compañía pero nunca deben ir en detrimento de las directivas de seguridad de la información que comprometan el sagrado compromiso de mantener la información de nuestros clientes confidencial; por lo que se entienden como excepciones:

- a) **ACTIVACIÓN DE PUERTOS USB Y/O ALGUNA UNIDAD ÓPTICA O DE ALMACENAMIENTO; PÁGINAS DE INTERNET O WEBMAIL:** Estas se pueden activar única y exclusivamente con permiso previo del jefe directo del área donde se realiza el proceso en el cual debe enviar un correo electrónico indicando el proceso a realizar y la duración del mismo que no puede ser superior a un día en el cual debe estar constantemente supervisado por el jefe directo y debe dejar evidencia de que fue lo que copio en la bitácora creada para tal fin; si la tarea es permanente se realizara comité de seguridad con el área de calidad, sistemas, el jefe directo del área solicitante y presidencia para evaluar la factibilidad de la solicitud y en caso de ser afirmativo se debe generar un acta con la descripción del proceso y los controles que se van a tomar frente a este evento de seguridad.
- b) **INGRESO A ÁREAS RESTRINGIDAS:** Estos ingresos deben estar sujetos a una aprobación por parte de los jefes de área de las dependencias donde se debe hacer el ingreso y estas deben estar soportadas por un correo electrónico dando el visto bueno o con una anotación en las bitácoras de ingreso a dependencias con acceso restringido.
- c) **INGRESO DE VISITAS A LA COMPAÑÍA:** Estas deben estar autorizadas por el jefe directo de la persona que interviene en el proceso, debe firmar el acta de ingresos que se encuentra en la recepción y su permanencia no debe ser mayor a media hora (Aplicar política de visitas).
- d) **SOLICITUD POR ENTIDAD JURÍDICA SOBRE EL HARDWARE:** Con la autoridad competente se debe realizar un backup de la información y después se debe realizar un borrado seguro de la información con la herramienta HardWipe con el método Gutmann de 35 Pasadas, llamar al contacto de la entidad con la cual se tiene el evento y no permitir que se saque ni el disco ni la torre de las instalaciones de RST Asociados S.A.S solo hasta que el encargado de la entidad del cliente de autorización después de que tenga en su poder la información del proceso que se realizó con la maquina en custodia.

CONTROL DE CAMBIOS		
VERSIÓN	DESCRIPCIÓN DE LA MODIFICACIÓN	FECHA ACTUALIZACIÓN
1.0	Emisión inicial.	07-Abr-2015
2.0	Inclusión de clasificación y fecha de actualización en control de cambios.	20-Jun-2018

Elaborado por: Director administrativo y director de T. I	Revisado por: Director administrativo y auditor interno	Aprobado por: presidente
Fecha: 29/02/2024	Fecha: 29/02/2024	Fecha: 29/02/2024

	POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Clasificación: 2
		Versión: 6.0
		Fecha de Actualización: 29/02/2024

3.0	Se realiza modificación en el numeral 2.4 Seguridad física en el Ítem a.	01-Mar-2021
4.0	Se realiza actualización documental	30-Mar-2022
5.0	Se realiza actualización documental	31-Jul-2023
6.0	Se realiza actualización documental, se confirma frecuencia de activación del plan de continuidad y realización de auditorias internas al SGC y SGSI.	29-Feb-2024

Elaborado por: Director administrativo y director de T. I	Revisado por: Director administrativo y auditor interno	Aprobado por: presidente
Fecha: 29/02/2024	Fecha: 29/02/2024	Fecha: 29/02/2024