ÍNDICE GENERAL

1 DESCRIPCIÓN DE LA POLÍTICA DE SEGURIDAD DE LAZZATE CIA. LTDA. COMO ENTIDAD CERTIFICADORA DE INFORMACIÓN Y SERVICIOS RELACIONADOS

Con la promulgación de la presente Política de Seguridad de la Información, Lazzate, formaliza su compromiso con el proceso de gestión responsable de información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de este importante activo.

1.1 POLITICA DE SEGURIDAD:

Acerca de la Seguridad de la Información

La seguridad de la información se entiende como la preservación, aseguramiento y cumplimiento de las siguientes características de la información:

Confidencialidad: los activos de información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.

Integridad: El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.

Disponibilidad: Los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que tengan los permisos adecuados.

Para ello es necesario considerar aspectos tales como:

Autenticidad: Los activos de información los crean, editan y custodian usuarios reconocidos quienes validan su contenido.

Posibilidad de Auditoría: Se mantienen evidencias de todas las actividades y acciones que afectan a los activos de información.

Protección a la duplicación: Los activos de información son objeto de clasificación, y se llevan registros de las copias generadas de aquellos catalogados como confidenciales.

No repudio: Los autores, propietarios y custodios de los activos de información se pueden identificar plenamente.

Legalidad: Los activos de información cumplen los parámetros legales, normativos y estatutarios de Lazzate.

Confiabilidad de la Información: Es fiable el contenido de los activos de información que conserven la confidencialidad, integridad, disponibilidad, autenticidad y legalidad.

1.2 ORGANIZACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN:

Lazzate garantiza el apoyo al proceso de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de la Seguridad de la Información, del cual hace parte integral la presente política, por medio de la creación de una comisión técnica denominada Comité de Seguridad de la Información cuya composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:

- Gerente General o un delegado especializado,
- Gerente de Tecnología o un delegado especializado,
- Jefe de Planificación de Proyectos o un delegado especializado,
- Jefe de la Red de Datos o un delegado especializado
- Asesor certificado en seguridad de la información.

En todo caso, dicha comisión o la mesa de trabajo, deberá revisar y actualizar anualmente esta política presentando las propuestas a las directivas de Lazzate para su aprobación mediante resolución o acto jurídico correspondiente.

Los jefes de departamento, previa identificación y valoración de sus activos de información, hacen parte del grupo de responsable de Seguridad de la Información y por tanto deben seguir los lineamientos de gestión enmarcados en esta política y en los estándares, normas, guías y procedimientos recomendados por el Comité de Seguridad de la Información y aprobados por la gerencia

1.3 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1.3.1 Generalidades.

La información es un recurso que, como el resto de los activos, tiene valor para Lazzate y por consiguiente debe ser debidamente protegida.

El establecimiento, seguimiento, mejora continua y aplicación de la Política de Seguridad de la Información garantiza un compromiso ineludible de protección a la misma frente a una amplia gama de amenazas. Con esta política se contribuye a minimizar los riesgos asociados de daño y se asegura el eficiente cumplimiento de las funciones sustantivas de la entidad apoyadas en un correcto sistema de información.

Lazzate establecerá los mecanismos para respaldar la difusión, estudio, actualización y consolidación tanto de la presente política como de los demás componentes del Sistema de Gestión de la Seguridad de la Información y alinearlos de forma efectiva con los demás sistemas de gestión.

1.3.2 Alcance.

Esta política se aplica en el conjunto de dependencias que componen Lazzate, a sus recursos, a la totalidad de los procesos internos o externos vinculados a Lazzate a través de contratos o acuerdos con terceros y a todo el personal de Lazzate, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

1.3.3 Objetivos.

Proteger, preservar y administrar objetivamente la información de Lazzate, junto con las tecnologías utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

Mantener la Política de Seguridad de la Información actualizada, vigente, operativa y auditada dentro del marco determinado por los riesgos globales y específicos de Lazzate para asegurar su permanencia y nivel de eficacia.

Definir las directrices de Lazzate para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento con el fin de garantizar la continuidad e integridad de los sistemas de información.

1.3.4 Responsabilidad.

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de Lazzate, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

La alta gerencia de Lazzate aprueba esta Política y es responsable de la autorización de sus modificaciones

El Comité de Seguridad de la Información de Lazzate es responsable de revisar y proponer a las directivas institucionales para su aprobación, el texto de la Política de Seguridad de la Información, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejora del Sistema de Gestión de Seguridad

de Lazzate. Es responsabilidad de dicho comité definir las estrategias de capacitación en materia de seguridad de la información.

El Coordinador del Comité de Seguridad de la Información será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento de la presente Política.

El grupo responsable de Seguridad Informática será responsable de cumplir funciones relativas a la seguridad de los sistemas de información de la entidad, lo cual incluye la operación del SGSI y supervisión del cumplimiento, dentro de la dependencia, de aspectos inherentes a los temas tratados en la presente Política. El nivel de supervisión que pueda realizar cada grupo responsable de seguridad está relacionado con el talento humano que lo conforma y en todo caso deberá ser aprobado por el Comité de Seguridad de la Información.

Los propietarios de activos de información son responsables de la clasificación, mantenimiento y actualización de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia. En general, tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

El jefe de Recursos Humanos cumplirá la función de notificar a todo el personal que se vincula contractualmente con Lazzate, de las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan del Sistema de Gestión de la Seguridad de la Información. De igual forma, será responsable de la notificación de la presente Política y de los cambios que en ella se produzcan a todo el personal, a través de la suscripción de los Compromisos de Confidencialidad y de tareas de capacitación continua en materia de seguridad según lineamientos dictados por el Comité de Seguridad de la Información.

Corresponde a la Gerencia de Tecnología determinar el inventario de activos de información y recursos tecnológicos de los cuales son propietarios o custodios, el cual será revisado y avalado por el área administrativa.

El jefe de la Oficina Jurídica verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la entidad con empleados y con terceros. Asimismo, asesorará en materia legal a la entidad en lo que se refiere a la seguridad de la información.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer y cumplir la Política de Seguridad de la Información vigente.

El personal de Control Interno es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos de información y la tecnología de información. Es su responsabilidad informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

1.4 IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE LOS ACTIVOS DIGITALES.

Cada dependencia, bajo supervisión del Comité de Seguridad de la Información, debe elaborar y mantener un inventario de los activos de información que poseen (procesada y producida). Las características del inventario, donde se incorpore la clasificación, valoración, ubicación y acceso de la información, las especifica el Comité de Seguridad de la Información, correspondiendo a la Gerencia de Tecnología brindar herramientas que permitan la administración del inventario por cada dependencia, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

1.4.1 Seguridad de la información en el Recurso Humano

Todo el personal de Lazzate, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe debe tener asociado un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. El área de tecnología debe mantener un directorio completo y actualizado de tales perfiles.

El Comité de Seguridad de la Información determina cuales son los atributos que deben definirse para los diferentes perfiles.

El Comité de Seguridad de la Información debe elaborar, mantener, actualizar, mejorar y difundir el manual de “Responsabilidades Personales para la Seguridad de la Información en Lazzate”.

La responsabilidad de custodia de cualquier archivo mantenido, usado o producido por el personal que se retira, o cambia de cargo, recae en el jefe de departamento o supervisor del contrato; en todo caso el proceso de cambio en la cadena de custodia de la información debe hacer parte integral del procedimiento de terminación de la relación contractual o de cambio de cargo.

1.4.2 Responsabilidades del personal de Lazzate

Todo el personal de Lazzate, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y las tareas que desempeñe debe firmar un acuerdo que contenga los términos y condiciones que regulan el uso de recursos de TI y las reglas y perfiles que autorizan el uso de la información institucional.

Los procedimientos para obtener tales perfiles y las características de cada uno de ellos deben ser mantenidos y actualizados por cada dependencia, de acuerdo a los lineamientos dados por la oficina de tecnología de la información, en cuanto a la información y la Red de Datos, en cuanto a los dispositivos hardware y los elementos software.

El Estatuto General y el reglamento interno deben contemplar procesos y sanciones disciplinarias para los casos en que se presente usos de información y TI que violen los términos y condiciones.

La Oficina de Recursos Humanos junto con la Oficina Tecnologías de la Información se encargarán de crear, actualizar, mantener y ejecutar un plan de capacitación en seguridad de la información que propenda por el crecimiento continuo de la conciencia individual y colectiva en temas de seguridad de la información.

La Gerencia de Tecnología en se encargará de crear y mantener un centro documental de acceso general con información relacionada con temas de seguridad de la información tales como responsabilidad en la administración de archivos, buenas prácticas, amenazas de seguridad, entre otros.

1.5 RESPONSABILIDADES DE LOS COLABORADORES.

Para poder usar los recursos de TI de Lazzate, los colaboradores deben leer y aceptar al momento de realizar el contrato laboral un acuerdo con los términos y condiciones. La Gerencia de Tecnología debe asegurar los mecanismos para la difusión y aceptación de dichas condiciones por medio de registros y manuales en línea.

El estatuto laboral debe contemplar procesos y sanciones disciplinarias para los casos en que se presente usos de información y TI que violen los términos y condiciones.

1.5.1 Responsabilidades de Usuarios Externos

Todos los usuarios externos y personal de empresas externas deben estar autorizados por un miembro del personal de Lazzate quien será responsable del control y vigilancia del uso adecuado de la información y los recursos de TI de Lazzate. Los procedimientos para el registro de tales usuarios deben ser creado y mantenido por la Gerencia de Tecnología en conjunto con la red de datos y la Oficina de Recursos Humanos.

Los usuarios externos deben aceptar por escrito los términos y condiciones de uso de la información y recursos de TI de Lazzate. Las cuentas de usuarios externos deben ser de perfiles específicos y tener caducidad no superior a tres (3) meses, renovables de acuerdo con la naturaleza del usuario.

1.5.2 Usuarios invitados y servicios de acceso público.

El acceso de usuarios no registrados solo debe ser permitido al sitio web de información comercial redistribuible. El acceso y uso a cualquier otro tipo de recurso de información y TI no es permitido a usuarios invitados o no registrados.

1.6 AUTENTICACIÓN DE USUARIOS Y CEREMONIA DE CLAVES

1.6.1 AUTENTICACIÓN MEDIANTE CONTRASEÑAS

1.6.1.1 Alta y baja de contraseñas.

Las gestiones asociadas a la creación o eliminación de contraseñas son responsabilidad de los administradores de los Servicios de Identidad Digital de Lazzate.

1.6.1.2 Sustitución de contraseñas.

El cambio de contraseñas podrá obedecer a:

- Cumplimiento del periodo de rotación establecido para la contraseña.

- Cambio de contraseña decidido por el usuario o el Departamento de Sistemas de Lazzate.

- Cambio de contraseña por olvido, pérdida o sospecha de haber sido comprometida la seguridad de la anterior.

- Cambio de una contraseña por defecto.

El responsable de iniciar un procedimiento de cambio de contraseña podrá ser el dueño de la cuenta cuya contraseña ha de cambiarse, o el Departamento de TI (responsable del Sistema) de Lazzate, y constará de los siguientes pasos:

1.6.1.3 Por decisión del usuario:

El usuario dispone de contraseña válida para acceder al servicio:

- Si el Servicio de Identidad Digital (SID) dispone de autoservicio de credenciales de autenticación, se seguirá el procedimiento específico del SID para gestionar el cambio de contraseña.

- Si el Servicio de Identidad Digital (SID) no dispone de autoservicio de credenciales de autenticación, contactará con el administrador del sistema de información para que haga uso de sus privilegios de administración y realice el cambio de contraseña

por una contraseña provisional, de un solo uso, que el usuario deberá sustituir en el inicio de la siguiente sesión.

- Si el usuario no dispone de contraseña válida para acceder al servicio: Contactará con el administrador del sistema de información para que haga uso de sus privilegios de administración y realice el cambio de contraseña por una contraseña provisional, de un solo uso, que el usuario deberá sustituir en el inicio de la siguiente sesión.

- Por decisión del Departamento de Sistemas (responsable del sistema).

- El administrador del sistema de información, haciendo uso de sus privilegios de administración, realizará el cambio de contraseña por una contraseña por una contraseña provisional, de un solo uso, que el usuario deberá sustituir en el inicio de la siguiente sesión.

1.6.1.4 Directiva de contraseñas

Todos los usuarios, independientemente del sistema de información para el que se definan o sean válidas, son responsables de sus contraseñas de acceso a servicios y de los accesos que se produzcan haciendo uso de dichas contraseñas.

En este sentido, se recomienda a los usuarios observar las siguientes indicaciones en cuanto a la custodia de sus contraseñas:

- No compartir sus contraseñas con otros usuarios.
- No anotar sus contraseñas ni introducirlas si alguien está observando.
- No enviar contraseñas por medios electrónicos o almacenarlas en ficheros de ordenador sin cifrar.

El usuario deberá custodiar sus contraseñas de forma efectiva siguiendo las directrices indicadas en la Normativa General de Utilización de los Recursos y Sistemas de Información de Lazzate

Los servicios de Identidad Digital de Lazzate, siempre que sea posible, deberán emplear herramientas de control que garanticen el cumplimiento de la Directiva de Contraseñas.

Todas las contraseñas asignadas a las cuentas activas en los sistemas de información de Lazzate deberán observar las restricciones que se detallan:

Parámetro Valor Periodo máximo de rotación:

- 30 días para cuentas de usuario.

- 90 días para cuentas de administración de sistemas.

Caducidad de contraseñas es automática, al finalizar el periodo máximo de rotación, excepto para contraseñas de administración de sistemas.

Reutilización de contraseñas: Ninguna de las 3 últimas.

Intervalo mínimo entre cambios: 2 días.

Longitud mínima: 8 caracteres.

Requisitos de complejidad:

• No contener en parte o en su totalidad el nombre de usuario.

• Estar compuesta por al menos 3 de entre los siguientes 4 conjuntos de caracteres: o Caracteres alfanuméricos en mayúsculas. o Caracteres alfanuméricos en minúsculas. o Caracteres numéricos. o Símbolos/caracteres especiales.

1.6.1.5 Semántica de contraseñas, se deberán evitar las contraseñas basadas en:

• Repetición de caracteres.

• Palabras del diccionario.

• Secuencias simples de letras, números o secuencias de teclado.

• Información fácilmente asociable al usuario como nombres de familiares o mascotas, números de teléfono, matrículas, fechas o en general información biográfica del usuario. Cautelas generales

1.6.1.6 Mantenerlas en secreto. Las contraseñas no deben compartirse con nadie.

Preferiblemente, las contraseñas iniciales deben ser entregadas en mano o a través de algún medio que no permita su acceso por personas no autorizadas. En el caso de enviarlas por medios telemáticos (correo electrónico, SMS, etc.) o en un soporte, se enviarán separadas del identificador.

Las contraseñas iniciales deben ser generadas automáticamente y se cambiarán en el primer acceso a los sistemas.

Los ficheros de contraseñas se deben almacenar con algún método de protección que garantice su confidencialidad e integridad (p. e. cifrado).
Los sistemas, no deben mostrar las contraseñas en claro por pantalla.

Todas las contraseñas por defecto de los sistemas o aplicaciones deben ser cambiadas o desactivadas cuando no sean necesarias.

La autenticación en los sistemas debe ser individual, no estando permitida la autenticación por grupo. Cuando sea necesario por razones operacionales, deberá estar justificado y aprobado formalmente, aplicando los controles de seguridad compensatorios necesarios.

El número de intentos de accesos sin éxito consecutivos debe estar limitado, tras el cual, se bloquearán los sistemas.

Los salvapantallas deben tener activada la protección por contraseña, bloqueándose tras un periodo de inactividad.

Cuando se considere necesario en servicios críticos, se contará con medidas adicionales a las establecidas en este Procedimiento.

No deben ser incluidas en correos electrónicos o en otros medios de comunicación electrónica ni comunicadas por teléfono.

No se deben escribir o almacenar contraseñas en texto claro o en formas fácilmente reversibles.

Se debe evitar la característica “Recordar Contraseña” existente en algunas aplicaciones y formularios.

Deben existir mecanismos de expiración y caducidad de contraseñas para obligar a los usuarios al cambio de esta.

Todas las contraseñas con privilegios especiales (administrador, root, etc.) deben cambiarse, al menos, cada 3 meses.

Todas las cuentas de usuario (acceso a sistema operativo, correo, servicios web, etc.) deben cambiarse, al menos, cada 6 meses.

Adicionalmente, deberán modificarse siempre que se sospeche que está comprometida a través de los procedimientos establecidos.

1.6.1.7 Factores del sistema de autenticación.

Un dato que el usuario debe conocer
Estará dado por la contraseña que cumple los parámetros antes solicitados.

Un objeto
Al inicio de sesión en los sistemas críticos se envía mediante OTP Telegram el código de aprobación de acceso al celular y usuario de Telegram registrado.

1.6.1.8 Gestión de inicios de sesión.

Se describen seguidamente los aspectos que deben tenerse en cuenta de cara a minimizar el número de accesos no autorizados a los sistemas.

- Hasta que no se haya completado con éxito el proceso de autenticación, no se deberá mostrar ningún tipo de información relativa al sistema (tal como identificadores del sistema o versiones de software instalado), que puedan ayudar a identificarlo, así como cualquier otro tipo de información que pueda facilitar su acceso no autorizado.

- Una vez se haya accedido correctamente al sistema, se deberá mostrar un mensaje que advierta que el uso del sistema sólo está permitido a usuarios autorizados.

- El acceso no autorizado está terminantemente prohibido y podrá ser objeto de acciones disciplinarias, sin perjuicio de las restantes acciones de naturaleza.

1.7 SEGURIDAD FÍSICA Y DEL ENTORNO

1.7.1 Acceso

Se debe tener acceso controlado y restringido a los cuartos de servidores principales, subsidiarios y a los cuartos de comunicaciones. La Gerencia de Tecnología elaborará y mantendrá las normas, controles y registros de acceso a dichas áreas.

1.7.2 Seguridad en los equipos

Los servidores que contengan información y servicios prioritarios deben ser mantenidos en un ambiente seguro y protegido por los menos con:

Controles de acceso y seguridad física.

Detección de incendio y sistemas de extinción de conflagraciones.

Controles de humedad y temperatura.

Bajo riesgo de inundación.

Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

Toda información institucional en formato digital debe ser mantenida en servidores aprobados por la Gerencia de Tecnología. No se permite la reubicación de información de carácter sensible y de Lazzate en servidores externos sin que medie una aprobación por escrito del Comité de Seguridad de la Información.

Equipos claves de comunicaciones deben se alimentados por sistemas de potencia eléctrica regulados y estar protegidos por UPS.

El departamento de TI debe asegurar que la infraestructura de servicios de TI se encuentre cubierta por mantenimiento y soporte adecuados de hardware y software Las estaciones de trabajo deben estar correctamente aseguradas y operadas por personal de Lazzate el cual debe estar capacitado acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información institucional.

Los medios que alojan copias de seguridad deben ser conservados de forma correcta de acuerdo con las políticas y estándares que para tal efecto elabore y mantenga el Comité de Seguridad en la Información.

Las dependencias tienen la responsabilidad de adoptar y cumplir las normas definidas para la creación y el manejo de copias de seguridad.

1.8 ADMINISTRACIÓN DE LAS COMUNICACIONES Y OPERACIONES

1.8.1 Reporte e investigación de incidentes de seguridad

El personal de Lazzate debe reportar con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad a través de su jefe de dependencia a la Gerencia de Tecnología. En casos especiales dichos reportes podrán realizarse directamente a la Gerencia General, la cual debe garantizar las herramientas informáticas para que formalmente se realicen tales denuncias.

El Comité de Seguridad de la Información debe preparar, mantener y difundir las normas, procesos y guías para el reporte e investigación de incidentes de seguridad.

En conformidad con la ley, Lazzate podrá interceptar o realizar seguimiento a las comunicaciones por diferentes mecanismos previa autorización del Comité de Informática y Telecomunicaciones, y en todo caso notificando previamente a los afectados por esta

decisión.

La Gerencia de Tecnología mantendrá procedimientos escritos para la operación de sistemas cuya no disponibilidad suponga un impacto alto en el desarrollo normal de actividades. A dichos sistemas se debe realizar seguimiento continuo del desempeño para asegurar la confiabilidad del servicio que prestan.

1.8.2 Protección contra software malicioso y hacking.

Todos los sistemas informáticos deben ser protegidos teniendo en cuenta un enfoque multi-nivel que involucre controles humanos, físicos técnicos y administrativos. El Comité de Seguridad de la Información elaborará y mantendrá un conjunto de políticas, normas, estándares, procedimientos y guías que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking.

Las estaciones de trabajo de Lazzate deben estar protegidas por software antivirus con capacidad de actualización automática en cuanto a firmas de virus. Los usuarios de las estaciones no están autorizados a deshabilitar este control.

Lazzate a través de la Gerencia de Tecnología podrá hacer seguimiento al tráfico de la red cuando se tenga evidencias de actividad inusual o detrimentos en el desempeño. La dependencia que realice dicho seguimiento deberá informar a la comunidad universitaria a través de correo electrónico o noticias en el portal institucional de la ejecución de esta tarea.

La Gerencia de Tecnología debe mantener actualizada una base de datos con alertas de seguridad reportadas por organismos competentes y actuar en conformidad cuando una alerta pueda tener un impacto considerable en el desempeño de los sistemas informáticos.

1.8.3 Protección contra software malicioso y hacking.

Toda información que pertenezca a la matriz de activos de información o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo con los procedimientos documentados por el Comité de Seguridad de la Información. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

Las dependencias de Lazzate deben realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas.

Los registros de copias de seguridad deben ser guardados en una base de datos creada para tal fin. La Gerencia de Tecnología debe proveer las herramientas para que las dependencias puedan administrar la información y registros de copias de seguridad. La Oficina de Control Interno debe efectuar auditorías aleatorias que permitan determinar el

correcto funcionamiento de los procesos de copia de seguridad.

Las copias de seguridad de información crítica deben ser mantenida de acuerdo a cronogramas definidos y difundidos al personal involucrado en dichos procesos.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios. Los usuarios deben entregar al respectivo jefe de dependencia las copias de seguridad para su registro y custodia.

1.8.4 Protección contra software malicioso y hacking.

La configuración de enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; debe ser documentada, respaldada por copia de seguridad y mantenida por la Gerencia de Tecnología Todo equipo de TI debe ser revisado, registrado y aprobado por la Gerencia de Tecnología antes de conectarse a cualquier nodo de la Red de comunicaciones y datos institucional. Dicha dependencia debe desconectar aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad a ser investigado.

1.8.5 Intercambio de Información con Organizaciones Externas.

Las peticiones de información por parte de entes externos de control deben ser aprobadas por la Gerencia de Tecnología y la Gerencia General, y dirigida por dichos entes a los responsables de su custodia.

1.8.6 Internet y Correo Electrónico

Las normas de uso de Internet y de los servicios de correo electrónico serán elaboradas, mantenidas y actualizadas por el Comité de Seguridad de la Información y en todo caso este comité debe velar por el cumplimiento del código de ética institucional y el manejo responsable de los recursos de Tecnologías de la Información.

1.8.7 Instalación de Software

Todas las instalaciones de software que se realicen sobre sistemas de Lazzate deben ser aprobadas por la Gerencia de Tecnología, de acuerdo a los procedimientos elaborados para tal fin por dichas dependencias.

No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor y relacionadas. La Gerencia de Tecnología debe desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad que debe ser investigado.

Corresponde a la Gerencia de Tecnología mantener una base de datos actualizada que contenga un inventario del software autorizado para su uso e instalación en los sistemas informáticos institucionales.

1.9 RESGUARDO DE INFORMACIÓN Y PLAN DE CONTINUIDAD DE LAZZATE CIA. LTDA.

El plan de continuidad de negocio de Lazzate Cia. Ltda., contempla el resguardo de información en ubicaciones diferentes teniendo una redundancia en los servicios prestados en caso de que se presente un acontecimiento de fuerza mayor o caso fortuito.

A continuación, se describe en todas su partes el plan de continuidad de la empresa:

1.9.1 PERSONAS OBLIGADAS A IMPLEMENTARLO:

El gerente de tecnología y el personal a cargo.
El personal administrativo que se vincule a los procesos informáticos derivados.

1.9.2 DEFINICIONES

1.9.2.1 Respaldo de Información:

Proceso mediante el cual, se realiza una copia exacta de la información contenida en una carpeta (previamente definida), en el disco duro de una computadora (PC o Laptop) asignada a un usuario de la red informática, y se actualiza mediante sincronizaciones cada 30 minutos.

1.9.2.2 Usuario de la Red Informática:

Personal de la organización, que tiene asignado cualquier equipo informático (PC o Laptop), que se encuentre bajo el dominio de la red o infraestructura informática, que produzca información técnica y operativa, relacionada con actividades organizacionales.

1.9.2.3 Servidor Informático tipo NAS:

Equipo electrónico destinado para el almacenamiento y gestión de la información o data informática, al cual se le introduce un programa o software especializado (DPM), para que ejecute rutinariamente la gestión de respaldo de la información y sincronización de esta, con todos los usuarios de la infraestructura informática de la organización.

1.9.2.4 Infraestructura Informática:

Son todos los equipos informáticos que se encuentran bajo el dominio de la organización

que gozan o comparten los servicios que se generan dentro de éste.

1.10 PROCEDIMIENTO PARA LA RECUPERACIÓN DE DESASTRES

La política de seguridad de Lazzate Cia. Ltda., determina que la CA recuperará la funcionalidad de sus sistemas en un plazo máximo de 48 horas.

Los servicios de revocación y presentación de listados de certificados revocados estarán disponibles en 24 horas.

1.10.1 CONTINUIDAD DE NEGOCIO DESPUÉS DE UN DESASTRE

Para efectos de la puesta en marcha después de un desastre la CA dispone de una localización alternativa para dar continuidad al negocio.

Los servicios primordiales como revocación y listados de certificados revocados deberán estar disponibles dentro de las siguientes 24 horas de sucedido el desastre o la emergencia.

1.10.2 INCIDENTES RELACIONADOS CON EL HARDWARE O SOFTWARE

A continuación, se detalla el procedimiento a seguir en relación con un incidente con el hardware o software:

1.10.2.1 Políticas de seguridad en el resguardo

- La programación de resguardo de la información y de las bases de datos deberá hacerse cada 15 minutos en el servidor, para procesos críticos.
- El resguardo medios ópticos será el viernes de cada semana al medio día y trasladada por la tarde a su sitio de custodia.
- El hardware y software deberá contar con un plan anual de mantenimiento preventivo y correctivo.
- El encargado de informática deberá garantizar el uso de los antivirus en cada equipo de trabajo.
- Cada 6 meses el usuario que tenga asignado computadora deberá realizar una limpieza de los archivos que no utilice, con la finalidad de liberar espacio en la estación de trabajo y en las carpetas compartidas el servidor.
- El empleado deberá hacer un uso adecuado de los equipos informáticos, cuidándolos de cualquier golpe, ralladura y derrame de cualquier líquido.
- Las cintas magnéticas o cualquier otro instrumento que resguarde la información deberán ser custodiada fuera de la matriz, en sitios y mecanismos que garanticen la seguridad de esta.
- La unidad de informática será la encargada de velar por el cumplimiento de esta

normativa.

- Cuando exista un despido o una renuncia de un empleado, la unidad de Recursos Humanos deberá informar inmediatamente al jefe de la unidad de informática, para que realice el bloqueo de la cuenta del usuario, a fin de evitar posibles eliminaciones o copias de información por parte del empleado que perjudique la información de la organización.

1.10.2.2 DESCRIPCIÓN DEL PROCEDIMIENTO

1.10.2.2.1 Respaldo a la Información generada mediante software.

Sistemas Específicos.
Bases de Datos.
Reloj de marcación.
Máquinas Virtuales.

1.10.2.2.2 Descripción de Procedimiento:

Este procedimiento se realiza utilizando un servidor informático tipo "NAS" y un software denominado Data Protección Manager "PM", el cual realiza copias fieles de la información almacenada por el usuario en una carpeta del equipo informático, mediante el cual el DPM realiza posterior a la copia 3 comparativa, sincronizaciones cada 30 minutos, a fin de mantener lo más cercano posible, la copia de la información en un 100%.

El proceso es continuo y permanente, siempre y cuando no exista una variante tecnológica. A continuación, se realizará una descripción paso a paso, del procedimiento antes descrito.

1.10.2.3 Procedimiento de Instalación, configuración y monitoreo de sistemas e infraestructura

1.10.2.3.1 Verificación de la compatibilidad:

Se debe comprobar si se cumplen los requisitos para la instalación en cuanto a hardware y software. Si es necesario se deben desinstalar las versiones antiguas del mismo software o complementos necesarios.

1.10.2.3.2 Verificación de la integridad:

Se verifica que el paquete de software es el original, esto se hace para evitar la instalación de programas maliciosos, es necesario comprobar el origen mediante el uso del antivirus.

1.10.2.3.3 Creación de los directorios requeridos:

Para mantener el orden en el directorio cada sistema operativo se debe tener un estándar para la instalación de ciertos archivos en ciertos directorios.

1.10.2.3.4 Creación de los usuarios requeridos:

Es necesario determinar los privilegios para cada usuario en función de sus actividades.

1.10.2.3.5 Concesión de los derechos requeridos:

Para ordenar el sistema y limitar daños en caso necesario, se les conceden a los usuarios solo el mínimo necesario de derechos.

Copia, desempaque y descompresión de los archivos desde el paquete de software:

Para ahorrar Ancho de banda y tiempo en la transmisión por internet o espacio de Disco duro, los paquetes vienen empacados y comprimidos.

Archivos principales, sean de fuente o binarios.
Archivos de datos, por ejemplo, datos, imágenes, modelos, documentos XML, etc.
Documentación
Archivos de configuración
Bibliotecas
Enlaces duros o enlaces simbólico a otros archivos

1.10.2.3.6 Compilación y enlace con las bibliotecas requeridas:

Para el caso de compilación de archivos mediante paquetes que se encuentren en biblioteca externas el usuario debe tener los permisos requeridos para acceder y realizar la descarga requerida.

1.10.2.3.7 Configuración:

Por medio de archivos de configuración se le da a conocer al software con que parámetros debe trabajar. Por ejemplo, los nombres de las personas que pueden usar el software, como verificar su clave de ingreso, la ruta donde se encuentran los archivos con datos o la dirección de nuestro proveedor de correo electrónico. Para sistemas complejos se debe desarrollar el Software Configuration Management.

1.10.2.3.8 Definir las variables de entorno requeridas

El usuario debe conocer dependiendo del nivel de privilegios estas variables con el fin de realizar las configuraciones necesarias.

1.10.2.3.9 Registro ante el dueño de la marca:

Contar con las licencias para el caso de software propietario.

Procedimientos de protección malicioso que permita detectar, prevenir y recuperarse de afectaciones de malware.
Como políticas de prevención los sistemas deben cumplir con lo siguiente:

1.10.2.3.10 Prevención basada en software

*Mantener un **programa antivirus actual**:* El antivirus debe ejecutarse de manera permanente para proteger al equipo de las amenazas de software maligno. Para que sea capaz de reconocer el mayor número posible de programas malintencionados, siempre debe estar a la orden del día por medio de actualizaciones automáticas.

*Un **firewall activo**:* Con el fin de eliminar accesos no deseados el cortafuegos debe permanecer siempre activo.

*Una **versión actual** del **sistema operativo**:* Se debe tener las actualizaciones automáticas siempre activas y realizar revisiones periódicas en sistemas operativos Linux.

***Versiones actuales** de los **programas**:* Actualizar las versiones de los navegadores, de Java, de Flash y de otras aplicaciones o complementos que contienen a menudo fallos de seguridad y permiten que el badware tenga acceso al sistema.

Uso prudente de aplicaciones de Internet:
Establecer ciertas directrices, se pueden disminuir notablemente las posibilidades de que el sistema se infecte:

- Instalar programas y archivos que procedan de **fuentes fiables**. El software y las actualizaciones deben descargarse siempre desde la página web del proveedor original y, en caso de freeware o shareware, la descarga debe realizarse desde portales serios y conocidos.
- Durante la instalación de programas descargados desde internet, lo debe realizar usuarios con privilegios y se deberá observar que al momento de realizar la instalación este no solicite la instalación de otros programas adicionales.
- No abrir ningún archivos o enlaces proveniente de correos electrónicos cuyos **remitentes no pertenezcan a la cadena de confianza.**
- Evitar interactuar con anuncios o banners durante la navegación.
- Manejar de forma adecuada el repositorio de claves.

1.10.2.3.11 Procedimiento de detección:

- Iniciar el equipo en **modo seguro.**
- Analizar el equipo con el **programa antivirus** actualizado.
- Analizar el equipo con un **software antimalware.**
- Eliminar malware del equipo mediante sistemas de emergencia o formateo.

1.10.2.3.12 La presencia de malware en páginas web

Medidas de seguridad en el alojamiento web

- Acceso cifrado al espacio web**:** usar o bien FTP sobre SSL (FTPS) o el protocolo SFTP.
- Nombres de usuario y contraseñas seguros**:**
- Autenticación de dos factores
- Actualización de CMS
- Copia de seguridad

1.10.2.3.13 Recuperación de software malicioso

Al momento de sufrir un ataque dentro del entrono web se deben realizar los siguientes pasos:

- Pasar a modo offline.
- Conectarse con el proveedor del ISP.
- Analizar el o los equipos desde los cuales se realizaron conexiones hacia el servicio web.
- Cambiar todas las contraseñas.
- Localizar daños y repararlos: es posible usar Google Search Console.
- Revisar el último backup.
- Eliminar la página web de las listas negra.

1.10.2.4 Procedimiento que contemplen el registro y protección de pistas de auditoría.

1.10.2.4.1 Responsabilidades y procedimientos:

- Se debe establecer una bitácora de registro de incidentes y el reporte de vulnerabilidades de la seguridad de la información, el monitoreo de los sistemas, las

alertas y las vulnerabilidades, se debería establecer y ejecutar un procedimiento para la gestión de incidentes.

- Identificar y clasificar los diferentes tipos de incidentes de seguridad de la información.
- Identificar y analizar las posibles causas de un incidente producido.
- Planificar e implementar acciones correctivas para evitar la recurrencia del incidente.
- Notificar a todos los funcionarios afectados por el incidente de la restauración del equipo, sistema servicio afectado, una vez esté solucionado el incidente.
- El Oficial de Seguridad de la Información, emitirá un reporte a los jefes de las áreas afectadas por el incidente.
- Recolectar y asegurar pistas de auditoría y toda la evidencia relacionada con el incidente.

1.10.2.4.2 Aprendizaje debido a los incidentes de seguridad de la información:

- La información que se obtiene de la evaluación de los incidentes de seguridad de la información se debe utilizar para identificar los incidentes recurrentes o de alto impacto.
- Determinar el número de incidentes por tipo, el número de incidentes graves, el tiempo medio de resolución de incidentes.
- Determinar el costo promedio por incidente.
- Determinar el número de incidentes recurrentes.
- Determinar la frecuencia de un incidente recurrente.

1.10.3 LOGS Y EVIDEENCIAS

Desarrollar y cumplir procedimientos internos cuando se recolecta y se presenta evidencia con propósitos de acción disciplinaria dentro de la institución.

Hay que asegurar que los sistemas de información cumplan con las normas legales para la producción de evidencia, para lograr la admisibilidad, calidad y cabalidad de esta.

Para lograr el peso de la evidencia, se debe demostrar la calidad y cabalidad de los

controles empleados para proteger correcta y consistentemente la evidencia (es decir, evidencia del control del proceso) en todo el periodo en el cual la evidencia por recuperar se almacenó y procesó, mediante un rastreo sólido de la evidencia.

En general, dicho rastreo sólido se puede establecer en las siguientes condiciones:

Se deberán tomar duplicados o copias de todos los medios removibles, la información en los discos duros o la memoria para garantizar la disponibilidad; es conveniente conservar el registro de todas las acciones durante el proceso de copiado y dichos procesos deberían tener testigos; y, el medio y los registros originales se deberán conservar intactos y de forma segura.

Se debe proteger la integridad de todo el material de evidencia. El proceso de copia del material de evidencia debe estar supervisado por personal de confianza y se debe registrar la información sobre cuándo y cómo se realizó dicho proceso, quién ejecutó las actividades de copiado y qué herramientas o programas se utilizaron.

1.11 GESTIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD

1.11.1 Reporte sobre los eventos de seguridad de la información

Instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente, que establezca la acción que se ha de tomar al recibir el reporte sobre un evento que amenace la seguridad de la información.

Establecer un punto de contacto (Oficial de Seguridad de la Información) para el reporte de los eventos de seguridad de la información. Es conveniente garantizar que este punto de contacto sea conocido en toda la organización, siempre esté disponible y puede suministrar respuesta oportuna y adecuada. Todos los empleados, contratistas y usuarios contratados por los proveedores deberán tener conciencia de su responsabilidad para reportar todos los eventos de seguridad de la información lo más pronto posible.

Cuando un incidente se produzca, el personal en turno responsable del equipo o sistema afectado debe realizar las siguientes acciones en su orden:

1.11.2 Identificar el incidente

- Registrar el incidente en una bitácora de incidentes (reporte de eventos) incluyendo fecha, hora, nombres y apellidos del personal en turno, departamento o área

afectada, equipo o sistema afectado y breve descripción del incidente.

- Notificar al Oficial de Seguridad de la Información de Lazzate Cia. Ltda.
- Clasificar el incidente de acuerdo con el tipo de servicio afectado y al nivel de severidad.
- Asignar una prioridad de atención al incidente en el caso de que se produjeran varios en forma simultánea.
- Realizar un diagnóstico inicial, determinando mensajes de error producidos, identificando los eventos ejecutados antes de que el incidente ocurra, recreando el incidente para identificar sus posibles causas.
- Escalar el incidente en el caso que el funcionario en turno no pueda solucionarlo, el escalamiento deberá ser registrado en la bitácora de escalamiento de incidentes. El funcionario en turno debe escalar el incidente a su jefe inmediato, en el caso en el que el funcionario no tuviere un jefe al cual escalarlo, este debe solicitar soporte al proveedor del equipo o sistema afectado.
- Investigar y diagnosticar en forma definitiva las causas por las cuales se produjo el incidente.
- Resolver y restaurar el servicio afectado por el incidente debido a la par de un equipo o un sistema, incluyendo un registro de la solución empleada en la bitácora de incidentes.
- Cerrar el incidente, actualizando el estado del registro del incidente en la bitácora de incidentes a "Resuelto". Confirmar con el funcionario en turno, responsable del equipo o del sistema de que el incidente ha sido resuelto.

1.11.3 Reporte sobre las debilidades en la seguridad

Todos los empleados, contratistas y usuarios de terceras partes deberán informar sobre estos asuntos a su director o directamente a su proveedor de servicio, tan pronto sea posible para evitar los incidentes de seguridad de la información. Los mecanismos de reporte deberán ser fáciles, accesibles y disponibles. Se les debe informar a ellos que, en ninguna circunstancia, deberán intentar probar una debilidad sospechada.

Cuando un empleado, contratista o usuario contratado por un proveedor detecte una vulnerabilidad o debilidad en un equipo, sistema o servicio deberá ejecutar las siguientes

acciones:

- Notificar a su jefe inmediato y este al Oficial de Seguridad de la Información de la debilidad o vulnerabilidad detectada.

- Registrar la fecha, hora, apellidos y nombres del funcionario que detectó la debilidad o vulnerabilidad, descripción de la debilidad, descripción de posibles incidentes de seguridad que pudieran ocurrir producto de esta debilidad. El responsable de llevar este reporte denominado

- "Reporte de vulnerabilidades o debilidades de la seguridad de la información" es el Oficial de Seguridad de la Información.

- Nunca, por razón alguna, deberá intentar probar la debilidad o vulnerabilidad detectada en la seguridad. El ensayo de las vulnerabilidades se podría interpretar como un posible uso inadecuado del sistema, equipo o servicio y también podría causar daño al sistema o servicio de información y eventualmente podría recaer en una responsabilidad legal.

- El Oficial de Seguridad de la Información deberá tomar las medidas pertinentes para prevenir o eliminar la vulnerabilidad o debilidad detectada.

1.12 CONTROL DE ACCESO

1.12.1 Categorías de Acceso

El acceso a los recursos de tecnologías de información de Lazzate debe estar restringida según los perfiles de usuario definidos por el Comité de Seguridad de la Información.

1.12.2 Control de Claves y Nombres de Usuario

El acceso a información restringida debe estar controlado. Se recomienda el uso de sistemas automatizados de autenticación que manejen credenciales o firmas digitales.

Corresponde a la Gerencia de Tecnología elaborar, mantener y publicar los documentos de servicios de red que ofrece Lazzate a su personal, colaboradores y terceros.

La Gerencia de Tecnología debe elaborar, mantener y publicar procedimientos de administración de cuentas de usuario para el uso de servicios de red.

El acceso a sistemas de cómputo y los datos que contienen es responsabilidad exclusiva del personal encargado de tales sistemas.

Lazzate debe propender por mantener al mínimo la cantidad de cuentas de usuario que el personal, los colaboradores, docentes y terceros deben poseer para acceder a los servicios de red.

El control de las contraseñas de red y uso de equipos es responsabilidad de la Gerencia de Tecnología. Dichas contraseñas deben ser codificadas y almacenadas de forma segura.

Las claves de administrador de los sistemas serán conservadas por la Gerencia de Tecnología y de la Información de Lazzate y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie. Se exceptúa de lo anterior las claves de administrador de servidores y equipos de escritorio adscritos a la Gerencia de Tecnología y de la Información las cuales deben ser conservadas por el Gerente de TI y el Gerente General y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie.

La Gerencia de Tecnología y de la Información debe elaborar, mantener y actualizar el procedimiento y las guías para la correcta definición, uso y complejidad de claves de usuario.

Como requisito para la terminación de relación contractual - o laboral - del personal de la Lazzate, la Gerencia de Tecnología y de la Información debe expedir un certificado de cancelación de las cuentas de usuario asignadas para el uso de recursos de Tecnologías de la Información de Lazzate.

1.12.3 Computación Móvil

Lazzate reconoce el alto grado de exposición que presenta la información y los datos almacenados en dispositivos portátiles (computadores portátiles, notebooks, PDA, celulares, etc). Corresponde a la Oficina de Recursos Humanos en conjunto con la Gerencia de Tecnología elaborar, mantener e implementar planes de capacitación que propendan por la formación y mantenimiento de la conciencia en cuestión de seguridad de la información.

Las redes inalámbricas potencialmente introducen nuevos riesgos de seguridad que deben ser identificados, valorados y tratados de acuerdo con los lineamientos de la Política de Seguridad en redes inalámbricas que debe elaborar el Comité de Seguridad de la Información.

1.12.4 Auditoria y Seguimiento

Todo uso que se haga de los recursos de Tecnologías de la Información en Lazzate debe ser seguidos y auditados de acuerdo con los lineamientos del Código de Ética y del Código de Uso de Recursos de Tecnologías de la Información, el cual debe ser elaborado por el

Comité de Seguridad de la Información.

1.12.5 Acceso Remoto

El acceso remoto a servicios de red ofrecidos por Lazzate debe estar sujeto a medidas de control definidas por la Gerencia de Tecnología, las cuales deben incluir acuerdos escritos de seguridad de la información

1.12.6 Adquisición, Desarrollo y Mantenimiento de Sistemas Software

Para apoyar los procesos operativos y estratégicos Lazzate debe hacer uso intensivo de las Tecnologías de la Información y las Comunicaciones. Los sistemas de software utilizados pueden ser adquiridos a través de terceras partes o desarrollados por personal propio.

La Gerencia de Tecnología debe elegir, elaborar, mantener y difundir el "Método de Desarrollo de Sistemas Software en Lazzate" que incluya lineamientos, procesos, buenas prácticas, plantillas y demás artefactos que sirvan para regular los desarrollos de software internos en un ambiente de mitigación del riesgo y aseguramiento de la calidad.

Todo proyecto de desarrollo de software interno debe contar con un documento de Identificación y Valoración de Riesgos del proyecto. Lazzate no debe emprender procesos de desarrollo – o mantenimiento – de sistemas software que tengan asociados riesgos altos no mitigados.

Los sistemas software adquiridos a través de terceras partes deben certificar el cumplimiento de estándares de calidad en el proceso de desarrollo.

1.13 ADMINISTRACIÓN DE CONTINUIDAD DE NEGOCIO DE LAZZATE CIA. LTDA.

La Administración de Continuidad del Negocio debe ser parte integral del Plan de Administración de Riesgo de Lazzate.

1.13.1 Cumplimiento

Todo uso y seguimiento de uso a los recursos de TI en Lazzate debe estar de acuerdo con las normas y estatutos internos, así como a la legislación nacional en la materia.

1.13.2 Términos y Definiciones

1.13.2.1 Información

Toda forma de conocimiento objetivo con representación física o lógica explícita.

1.13.2.2 Activo de Información

Datos o información propiedad de Lazzate que se almacena en cualquier tipo de medio y que es considerada por la misma como sensitiva o crítica para el cumplimiento de los objetivos misionales.

1.13.2.3 Establecer matriz de información crítica

1.13.2.3.1 Sistema de Información

Conjunto ordenado de elementos cuyas propiedades se relacionan e interaccionan permitiendo la recopilación, procesamiento, mantenimiento, transmisión y difusión de información utilizando diferentes medios y mecanismos tanto automatizados como manuales.

1.13.2.3.2 Propietario de Activos de Información

En el contexto de la norma NTC 27001, un propietario de activos de información es cualquier persona o entidad a la cual se le asigna la responsabilidad formal de custodiar y asegurar un activo de información o un conjunto de ellos.

1.13.2.3.3 Tecnología de la Información

Conjunto de hardware y software operados por la entidad - o por un tercero en su nombre, que componen la plataforma necesaria para procesar y administrar la información que requiere la entidad para llevar a cabo sus funciones.

1.13.2.3.4 Evaluación de Riesgos

Evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de esta, la probabilidad de que ocurran y su potencial impacto

1.13.2.3.5 Administración de Riesgos

Proceso de identificación, control y reducción o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

1.13.2.3.6 Comité de Seguridad de la Información

El Comité de Seguridad de la Información, es un cuerpo integrado por diferentes representantes de Lazzate, destinado a garantizar el apoyo manifiesto de las directivas a las iniciativas de seguridad. Su función principal es definir, estructurar, recomendar, hacer

seguimiento y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI) de Lazzate. Depende directamente de la Gerencia General, y complementa el trabajo de la Gerencia de Tecnología sirviendo como consultor técnico en temas relacionados con la seguridad de la información.

1.13.2.3.7 Responsable de Seguridad Informática

Coordinador general del Comité de Seguridad de la Información. Su función principal es supervisar el cumplimiento de la presente Política y los lineamientos del SGSI.

1.13.2.3.8 Grupo responsable de Seguridad Informática

Grupos de apoyo creado en dependencias de Lazzate que manejan información sensible o crítica y que se encargan de velar por la operación del SGSI. Están conformados por funcionarios o contratistas de la dependencia que tengan formación en temas de seguridad de la información.

1.13.2.3.9 Incidente de Seguridad Informática

Un incidente de seguridad informática es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad, disponibilidad, legalidad o confiabilidad de la información.

Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

1.13.2.3.10 Cadena de custodia

En el ámbito de la seguridad de la información La cadena de custodia es la aplicación de una serie de normas y procedimientos tendientes a asegurar, depositar y proteger cada activo de información para evitar la pérdida de integridad, disponibilidad o confidencialidad.

1.14 PLAN DE CESE DE LAZZATE CIA. LTDA.

El articulo 35. de la Ley de Comercio Electrónico vigente en el Ecuador, que todos los Entes de Certificación deberán notificar al organismo de control, por lo menos con noventa días de anticipación, la cesación de sus actividades y se sujetarán a las normas y procedimientos establecidos en los reglamentos que se dicten para el efecto.

En función a lo que instruye la ley vigente, y con el fin de minimizar las afectaciones a sus usuarios y Terceros Vinculados, Lazzate implementará los procesos que se detallan a continuación:

1.14.1 CESE DE LA CA

- Notificar al organismo de control (ARCOTEL), con por lo menos 90 días de anticipación, sobre el cese de actividades.
- Notificar a sus usuarios, suscriptores y Terceros Vinculados, con por lo menos 90 días de anticipación, sobre el cese de actividades.
- Realizar por lo menos una publicación dirigida a sus usuarios y Terceros Vinculados, informando del cese de actividades, en nuestro portal web y diferentes redes sociales que maneje Lazzate.
- Dar por terminados todos los contratos de Tercera Vinculación con entidades que utilicen nuestra CA.
- La CA dejará de emitir certificados.
- Eliminar todas las claves privadas de la CA.
- Revocar todos los certificados que se hubieren emitido con nuestra CA.
- Todos los registros y archivos digitales de la CA serán transferidos a un custodio seleccionado por la CA.

1.14.2 CESE DE LA RA

En los casos que una Autoridad de Registro determine la necesidad de cesar sus funciones, se seguirá el siguiente procedimiento:

- Deberá notificar con 60 días de anticipación su voluntad de cese de actividades.
- Una vez recibida la notificación deberá dejar de emitir y renovar certificados.
- Deberá revocar los certificados emitidos a favor de dicho Tercer Vinculado.
- Prestará toda su voluntad y colaboración para que el equipo técnico y auditor de Lazzate pueda verificar que el cese se llevo a cabo bajo los lineamientos específicos requeridos por Lazzate.

1.15 CERTIFCACIONES

Lazzate garantiza la prestación del servicio basado en las certificaciones internacionales listadas a continuación, a las que damos cumplimiento en conjunto con nuestros

proveedores

1.15.1 Formatos de Firmas

Creación y Verificación de Productos de Firma Electrónica de Ascertia

PDF (ISO 32000), PDF/A (ISO 19005), PAdES (ETSI TS 102 778, EN 319 142-1 and EN 319 142-2) firmas

Firma Visible
Firma Invisible
Firma Certificada de Autor
Aprobación de Firmas
Adobe® CDS Signatures
PAdES Parte 2 (Básico)
PAdES Parte 3 (Mejorado)
PAdES Parte 4 (Larga Duración)

XML (W3C), XAdES (ETSI TS 101 903, EN 319 132-1 and EN 319 132-2) firmas

XML DSig
XAdES-EPES
XAdES2-BES
XAdES-T
XAdES-C
XAdES-X (Type 2)
XAdES-X-L
XAdES-A

CMS, PKCS#7, CAdES (ETSI TS 101 733, EN 319 122-1 and EN 319 122-2) firmas

CMS/PKCS#7/ and S/MIME
CAdES-BES
CAdES-EPES
CAdES-T
CAdES-C
CAdES-X-L
CAdES-A

Además de dar cumplimiento a las certificaciones ISO 9001:2015 y 27001:2013, que se adjuntan como Anexo 3.

1.16 POLITICA CRIPTOGRAFICA DE LAZZATE CIA. LTDA.

1.16.1 Generalidades

Con el fin de garantizar la confidencialidad e integridad de algunos documentos designados como sensibles, LAZZATE CIA. LTDA. debe utilizar sistemas y técnicas criptográficas para la protección de la información.

El sistema de información debe implementar mecanismos de protección de información que cumplan con la reglamentación, políticas, estándares, guías aplicables, así como:

Proporcionar una protección adecuada a los equipos utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.
Proteger las claves secretas y privadas evitando sean copiadas o modificadas sin autorización.

LAZZATE CIA. LTDA., deberá velar porque la información de su custodia o propiedad que es catalogada como pública o confidencial se cifre al momento de almacenarse o transmitirse por cualquier medio. Para dar cumplimiento al tratamiento definido para los activos de información, todos los involucrados en el alcance deben cumplir, las siguientes directrices:

1.16.2 Directrices de seguridad para todo el personal:

En concordancia con el compromiso de la empresa a continuación se detallan las directrices para todo el personal, sobre los cuales se regirá la aplicación de la presente política:

La información que contenga contraseñas de usuario o claves para el control de acceso a los sistemas de información no podrá ser almacenada en texto plano y deberá hacer uso de mecanismos criptográficos.

Todos los documentos que se han cifrado y descifrado, en caso de que se requiera, deberán ser almacenados y tratados con las medidas de seguridad requeridas conforme al grado de clasificación de la información.

Se deberá identificar todo sistema de información que requiera realizar transmisión de información pública o confidencial, para así garantizar que cuente con mecanismos de cifrado de datos.

Se deberán cifrar los discos duros de los equipos de cómputo que contengan información pública o confidencial.

El manejo de llaves criptográficas se debe realizar de acuerdo con los lineamientos establecidos en las Directrices de Llaves/Claves Criptográficas.

1.16.3 Directrices de Llaves/Claves Criptográficas

LAZZATE CIA. LTDA., vela porque la información que custodie o de la cual sea propietaria, y que se encuentre catalogada como pública o confidencial, sea cifrada al momento de almacenarse y transmitirse por cualquier medio.

El administrador del sistema informático será la persona responsable y encargada de la activación, recepción, protección de las llaves/claves criptográficas públicas y privadas según sea la necesidad de LAZZATE CIA. LTDA., además deberá proteger todas las llaves/claves contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada.

El Administrador del sistema informático, deberá generar claves para diferentes sistemas criptográficos y diferentes aplicaciones incluyendo fechas de inicio y caducidad de las claves, así como generar y obtener certificados de claves públicas.

Los responsables de las llaves/claves criptográficas deberán almacenar las llaves de forma segura y se comprometerán a restringir el acceso sólo a los usuarios autorizados. De igual forma, una copia de las llaves deberá ser almacenada en sitio seguro para su recuperación en caso tal que esta se extravíe.

El cambio o actualización de las llaves/claves deberá ser solicitado por el personal responsable o quien haga su uso.

El oficial de seguridad de la información deberá incorporar funcionalidad para recuperar claves perdidas o corruptas como parte de la gestión de continuidad de los servicios informáticos.

Las llaves/claves serán revocadas y/o destruidas si lo considera pertinente el oficial de seguridad de la información o persona delegada, cuando exista sospecha de que pudieron ser accedidas por una persona no autorizada o cuando el colaborador culmine su relación con LAZZATE CIA. LTDA.

Para todas y cada una de las actividades pertenecientes a la administración, gestión y eliminación de las llaves/claves criptográficas, se deberá mantener registro de las actividades realizadas en una bitácora a manera de reporte.

Los sistemas que actualmente cuenten con algún mecanismo de cifrado deberán acogerse a la presente política.

Todos los servidores utilizaran comunicaciones mediante certificación SSL, las mismas que se renuevan cada año, para garantizar la integridad, confidencialidad y autenticidad de las conexiones a los servicios, información o datos que se trasmitan a través de los aplicativos y de la página institucional con un algoritmo de encriptación de hash SHA-2 128 y/o 256 bits.

1.16.4 Directrices de seguridad para el personal que trata información de LAZZATE CIA. LTDA.

Se deberán cifrar los documentos lógicos, cuando contengan información pública o confidencial, en particular los documentos importantes de LAZZATE CIA. LTDA.

Se deberán cifrar o aplicar claves a los documentos (pdf, excel, word, bd, csv, etc.) que contengan datos personales o datos sensible.

La entrega de la clave del documento debe realizarse a través de un medio diferente al del envío del archivo.

Directrices de seguridad para el personal encargado de la configuración.

Deberá definir, configurar y administrar el sistema de cifrado, así como velar por el cumplimiento de la presente política y generar los reportes que se requieran.

El personal de LAZZATE CIA. LTDA., deberá:

- Firmar digitalmente toda documentación interna y externa.
- Debe Capacitar al personal sobre la firma, verificación y validación de documentos.
- Monitorear el buen uso de la firma Electrónica dentro de las competencias laborales.

1.16.5 Incumplimiento

El incumplimiento de esta política de seguridad y privacidad de la información traerá consigo las consecuencias legales que apliquen a la normativa de LAZZATE CIA. LTDA., incluyendo lo establecido en las normas que competen al Gobierno Ecuatoriano en cuanto dicta la LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA Art.23 TITULO SEXTO. Siendo la
Unidad de Talento Humano la encargada de vigilar y controlar la sanción correspondiente

al incumplimiento de esta política.

1.16.6 Responsabilidades

Oficial de Seguridad de la Información:
Velar por el cumplimiento de la presente política para garantizar que la información reservada y clasificada se cifre en el momento de almacenarse o transmitirse por cualquier medio.

Director de la Unidad de Tecnologías de la Información y Comunicaciones:
Garantizar que todo sistema de información que requiera realizar transmisión de información pública o confidencial cuente con mecanismos de cifrado de datos. Para este propósito deberá proveer los métodos de cifrado de la información que se requieran.

Responsable de Seguridad Informática:
Monitorear el uso de sistemas criptográficos, llaves criptográficas, certificados SSL, firmas electrónicas y sistemas de validación criptográficos de la LAZZATE CIA. LTDA.

Personal:
Garantizar el cifrado de la información pública o confidencial que traten dentro del desarrollo de sus actividades para con LAZZATE CIA. LTDA.

Información pública:
Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado. Art. 5 Información Confidencial: Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 (66) y 24 (76) de la Constitución Política de la República. Art. 6

Llaves criptográficas:
Son códigos (algoritmos) que se generan de forma automática y se guarda en un directorio especial durante la instalación. Habitualmente, esta información es una secuencia de números o letras mediante la cual, en criptografía, se especifica la transformación del texto plano en texto cifrado, o viceversa.

Personal:
Es aquella persona que tiene una relación con LAZZATE CIA. LTDA., directa o a través de un tercero, bajo cualquier tipo de vinculación: empleado, contratistas, proveedores,

estudiantes en práctica, etc.

Texto plano:
Es un archivo informático que contiene únicamente texto formado solo por caracteres que son legibles por humanos, careciendo de cualquier tipo de formato tipográfico. También son llamados archivos de texto llano, simple o sin formato.